SUSE LINUX Enterprise Server

Installation und Administration

9. Auflage 2004

Copyright ©

Dieses Werk ist geistiges Eigentum der SUSE LINUX AG.

Es darf als Ganzes oder in Auszügen kopiert werden, vorausgesetzt, dass sich dieser Copyrightvermerk auf jeder Kopie befindet.

Alle in diesem Buch enthaltenen Informationen wurden mit größter Sorgfalt zusammengestellt. Dennoch können fehlerhafte Angaben nicht völlig ausgeschlossen werden. Die SUSE LINUX AG, die Autoren und die Übersetzer haften nicht für eventuelle Fehler und deren Folgen.

Die in diesem Buch verwendeten Soft- und Hardwarebezeichnungen sind in vielen Fällen auch eingetragene Warenzeichen; sie werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Die SUSE LINUX AG richtet sich im Wesentlichen nach den Schreibweisen der Hersteller. Die Wiedergabe von Waren- und Handelsnamen usw. in diesem Buch (auch ohne besondere Kennzeichnung) berechtigt nicht zu der Annahme, dass solche Namen (im Sinne der Warenzeichen und Markenschutz-Gesetzgebung) als frei zu betrachten sind.

Hinweise und Kommentare richten Sie an `documentation@suse.de`.

Autoren:	Stefan Behlert, Frank Bodammer, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Torsten Duwe, Thorsten Dubiel, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Carsten Groß, Joachim Gleißner, Andreas Grünbacher, Franz Hassels, Andreas Jaeger, Klaus Kämpf, Hubert Mantel, Lars Marowsky-Bree, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Peter Pöml, Thomas Renninger, Heiko Rommel, Marcus Schäfer, Nicolaus Schüler, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz
Redaktion:	Jörg Arndt, Karl Eichwalder, Antje Faber, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Ines Pozo, Thomas Rölz, Thomas Schraitle
Layout:	Manuela Piotrowski, Thomas Schraitle
Satz:	DocBook-XML, LaTeX

Dieses Buch ist auf 100 % chlorfrei gebleichtem Papier gedruckt.

Inhaltsverzeichnis

I Installation **5**

1 Installation mit YaST **7**

1.1 S/390, zSeries: Systemstart zur Installation 8

1.2 Systemstart zur Installation 8

1.2.1 Mögliche Probleme beim Systemstart 8

1.3 Startbildschirm 10

1.4 Sprachauswahl 13

1.5 S/390, zSeries: Konfiguration der Festplatten 14

1.6 Installationsmodus 15

1.7 Installationsvorschlag 16

1.7.1 Installationsmodus 17

1.7.2 Tastaturlayout 17

1.7.3 Maus 18

1.7.4 Partitionierung 18

1.7.5 Experten-Partitionierung mit YaST 24

1.7.6 Software 31

1.7.7 System-Start (Bootloader-Installation) 34

1.7.8 Zeitzone 35

1.7.9 Sprache 35

1.7.10 Installation durchführen 36

1.7.11 S/390, zSeries: IPL des installierten Systems 37

1.7.12 s390, zseries: Verbindungsaufbau nach dem IPL . . . 37
1.8 Installation abschließen . . . 39
1.8.1 Root-Passwort . . . 39
1.8.2 Netzwerkkonfiguration . . . 40
1.8.3 Internet-Verbindung testen . . . 41
1.8.4 Software-Updates laden . . . 42
1.8.5 Netzwerkdienste . . . 43
1.8.6 Benutzer-Authentifizierung . . . 44
1.8.7 Konfiguration als NIS-Client . . . 44
1.8.8 Lokale Benutzer anlegen . . . 46
1.8.9 Release-Notes lesen . . . 48
1.9 Hardware-Konfiguration . . . 48
1.10 Grafisches Login . . . 50

2 YaST – Konfigurationen 51
2.1 Der Start von YaST . . . 52
2.1.1 Start über eine grafische Oberfläche . . . 52
2.1.2 Start über ein entferntes Terminal . . . 52
2.2 Das YaST-Kontrollzentrum . . . 53
2.3 Software . . . 53
2.3.1 Installationsquelle wechseln . . . 53
2.3.2 YaST-Online-Update . . . 54
2.3.3 Patch-CD-Update . . . 58
2.3.4 Software installieren oder löschen . . . 59
2.3.5 System-Update . . . 68
2.3.6 SUSE Software Development Kit 9 (SDK) . . . 72
2.4 Hardware . . . 73
2.4.1 CD-ROM-Laufwerke . . . 73
2.4.2 S/390, zSeries: DASD . . . 74
2.4.3 Drucker . . . 74
2.4.4 Festplatten-Controller . . . 80
2.4.5 Grafikkarte und Monitor (SaX2) . . . 81

2.4.6 Hardware-Informationen 92
2.4.7 IDE DMA-Modus 92
2.4.8 Maus 93
2.4.9 Scanner 93
2.4.10 Sound 95
2.4.11 S/390, zSeries: ZFCP 97
2.5 Netzwerkgeräte 98
2.6 Netzwerk-Dienste 98
2.6.1 DHCP-Server 98
2.6.2 Hostname und DNS 98
2.6.3 NFS-Client und NFS-Server 98
2.6.4 Konfiguration eines Samba-Servers 98
2.6.5 Konfiguration eines Samba-Clients 99
2.6.6 NTP Client 99
2.6.7 Routing 100
2.6.8 Mail Transfer Agent 100
2.6.9 Mailserver 101
2.6.10 Netzwerkdienste (inetd) 102
2.7 Sicherheit und Benutzer 103
2.7.1 Benutzerverwaltung 103
2.7.2 Gruppenverwaltung 104
2.7.3 Einstellungen zur Sicherheit 105
2.7.4 Firewall 107
2.8 System 109
2.8.1 Sicherungkopie der Systembereiche 109
2.8.2 System wiederherstellen 109
2.8.3 Erstellen einer Boot-, Rettungs- oder Moduldiskette . 110
2.8.4 Bootloader-Konfiguration 113
2.8.5 LVM 113
2.8.6 EVMS 113
2.8.7 Partitionieren 114
2.8.8 Profilmanager (SCPM) 114

2.8.9 Runlevel-Editor 114
2.8.10 Sysconfig-Editor 116
2.8.11 Zeitzone auswählen 116
2.8.12 Sprache auswählen 116
2.8.13 Tastaturlayout auswählen 117
2.9 Sonstiges 117
2.9.1 Eine Support-Anfrage stellen 117
2.9.2 Startprotokoll 118
2.9.3 Systemprotokoll 118
2.9.4 Treiber-CD des Herstellers laden 119
2.10 YaST im Textmodus (ncurses) 119
2.10.1 Navigation innerhalb der YaST-Module 120
2.10.2 Einschränkung der Tastenkombinationen 122
2.10.3 Aufruf der einzelnen Module 122
2.10.4 Das YaST Online Update 122

3 Besondere Installationsvarianten 125
3.1 linuxrc 126
3.1.1 Die Grundlage: linuxrc 126
3.1.2 Hauptmenü 126
3.1.3 System-Information 127
3.1.4 Laden von Modulen 128
3.1.5 Parametereingabe 129
3.1.6 System / Installation starten 131
3.1.7 Mögliche Probleme 132
3.1.8 Parameter an linuxrc übergeben 134
3.2 Installation per VNC 136
3.2.1 Vorbereitungen zur VNC-Installation 136
3.2.2 Clients zur VNC-Installation 137
3.3 Textbasierte Installation mit YaST 137
3.4 SUSE LINUX starten 139
3.4.1 Der grafische SUSE-Bildschirm 139

3.4.2 SUSE-Bildschirm deaktivieren 140
3.5 Besondere Installationen 140
3.5.1 Automatische Installation mit Autoyast 140
3.5.2 Installation via Netzwerk 141
3.6 x86: Tipps und Tricks 141
3.6.1 Bootdiskette unter DOS erstellen 141
3.6.2 Bootdiskette unter unix-artigem System erstellen . . 143
3.6.3 Booten von Diskette (SYSLINUX) 144
3.6.4 CD 2 zum Booten verwenden 145
3.6.5 Unterstützt Linux mein CD-ROM-Laufwerk? 145
3.7 x86: ATAPI-CD-ROM bleibt beim Lesen hängen 146
3.8 SCSI-Geräte und dauerhafte Gerätedateinamen 147
3.9 Partitionieren für Fortgeschrittene 148
3.9.1 Die Größe der Swap-Partition 149
3.9.2 Partitionierungsvorschläge für spezielle Szenarien . 149
3.9.3 Optimierungsmöglichkeiten 150
3.10 LVM-Konfiguration 152
3.10.1 Logical Volume Manager (LVM) 153
3.10.2 Konfiguration des LVM mit YaST 154
3.10.3 LVM – Partitionierer 155
3.10.4 LVM – Einrichtung der Physical Volumes 157
3.10.5 Logical Volumes 158
3.11 Soft-RAID 160
3.11.1 Gängige RAID-Level 161
3.11.2 Soft-RAID-Konfiguration mit YaST 162
3.12 Massenspeicher über IP-Netzwerke – iSCSI 163

4 Zentrale Softwareinstallation und -aktualisierung 165
4.1 Einrichtung eines zentralen Installationsservers 166
4.1.1 Konfiguration mit YaST 166
4.1.2 Client-Installation über den Installationsserver 168
4.2 Softwareupdates mit dem YOU-Server verwalten 170
4.2.1 Konfigurieren des lokalen YOU-Servers 170
4.2.2 Konfigurieren der Clients 172
4.3 Booten vom Netz 173
4.3.1 Konfiguration des tftpd 173
4.3.2 Einrichten des dhcpd 175
4.3.3 Start des Bootvorgangs 176

5 Update des Systems und Paketverwaltung 177
5.1 SUSE LINUX aktualisieren 178
5.1.1 Vorbereitungen 178
5.1.2 Mögliche Probleme 179
5.1.3 Update mit YaST 180
5.1.4 Manuell gesteuertes Update 181
5.2 Softwareänderungen von Version zu Version 183
5.2.1 Von SLES8 auf SLES9 184
5.3 RPM – Der Paket-Manager der Distribution 190
5.3.1 Prüfen der Authentizität eines Pakets 191
5.3.2 Pakete verwalten 192
5.3.3 RPM und Patches 194
5.3.4 Anfragen stellen 196
5.3.5 Quellpakete installieren und kompilieren 198
5.3.6 RPM-Pakete mit build erzeugen 200
5.3.7 Tools für RPM-Archive und die RPM-Datenbank . . 201

6 Systemreparatur **203**
6.1 Starten der YaST-Systemreparatur 204
6.2 Automatische Reparatur 205
6.3 Benutzerdefinierte Reparatur 206
6.4 Expertenwerkzeuge 207
6.5 S/390, zSeries: Die initrd als Rettungssystem 208
6.5.1 IPL des Rettungssystems 209
6.5.2 Laden der DASD-Module 210
6.5.3 Mounten des Rootdevices 211
6.5.4 Wechsel in das gemountete Dateisystem 212
6.5.5 Ausführen von zipl 212
6.5.6 Verlassen des Rettungssystems 212

II System **215**

7 32-bit und 64-bit Applikationen in einer 64-bit Systemumgebung **217**
7.1 Laufzeit-Unterstützung 218
7.2 Softwareentwicklung 219
7.3 Software-Kompilierung auf Biarch-Plattformen 220
7.4 Kernel-Spezifika 222

8 Booten und Bootmanager **223**
8.1 Der Bootvorgang auf dem PC 224
8.1.1 Master Boot Record 224
8.1.2 Bootsektoren 224
8.1.3 Booten von DOS oder Windows 225
8.2 Bootkonzepte 225
8.3 Map Files, GRUB und LILO 226
8.4 Booten mit GRUB 227
8.4.1 Das GRUB-Bootmenü 228
8.4.2 Die Datei device.map 234
8.4.3 Die Datei /etc/grub.conf 235

8.4.4 Bootpasswort setzen . . . 236
8.4.5 Mögliche Probleme und weitere Informationen . . . 237
8.5 Booten mit LILO . . . 238
8.5.1 Grundlagen . . . 238
8.5.2 LILO-Konfiguration . . . 240
8.5.3 Der Aufbau der Datei lilo.conf . . . 240
8.5.4 Installation und Deinstallation von LILO . . . 244
8.6 Bootloader-Konfiguration mit YaST . . . 244
8.6.1 Das Hauptfenster . . . 245
8.6.2 Optionen der Bootloader-Konfiguration . . . 247
8.7 Linux-Bootloader entfernen . . . 249
8.7.1 MBR wiederherstellen (DOS/Win9x/ME) . . . 249
8.7.2 MBR wiederherstellen (Windows XP) . . . 250
8.7.3 MBR wiederherstellen (Windows 2000) . . . 250
8.8 Für alle Fälle: Boot-CD erstellen . . . 250
8.8.1 Boot-CD mit ISOLINUX . . . 250
8.9 S/390, zSeries: Der Bootloader ZIPL . . . 252
8.9.1 Verwendung . . . 252

9 Der Linux Kernel 255
9.1 Kernel-Update . . . 256
9.2 Die Kernelquellen . . . 257
9.3 Konfiguration des Kernels . . . 257
9.3.1 Kommandozeilenkonfiguration . . . 258
9.3.2 Konfiguration im Textmodus . . . 258
9.3.3 Konfiguration unter dem X Window System . . . 258
9.4 Kernel-Module . . . 259
9.4.1 Erkennung der akutellen Hardware mit hwinfo . . . 259
9.4.2 Umgang mit Modulen . . . 260
9.4.3 /etc/modprobe.conf . . . 261
9.4.4 Kmod – der Kernel Module Loader . . . 261
9.5 Einstellungen bei der Kernelkonfiguration . . . 262
9.6 Übersetzen des Kernels . . . 262
9.7 Kernel installieren . . . 263
9.8 Festplatte nach der Übersetzung aufräumen . . . 265

10 Systemmerkmale **267**
10.1 Linux-Standards 268
10.1.1 Linux Standard Base (LSB) 268
10.1.2 Filesystem Hierarchy Standard (FHS) 268
10.1.3 teTeX — TeX unter SuSE Linux 268
10.1.4 Zu FTP 268
10.1.5 Zu HTTP 269
10.2 Hinweise zu speziellen Softwarepaketen 269
10.2.1 Paket bash und /etc/profile 269
10.2.2 Paket cron 270
10.2.3 Protokoll-Dateien — das Paket logrotate 270
10.2.4 Manual-Pages 271
10.2.5 Der Befehl ulimit 272
10.2.6 Der Befehl free 273
10.2.7 Die Datei /etc/resolv.conf 273
10.2.8 Einstellungen für GNU Emacs 274
10.3 Booten mit der initial ramdisk 275
10.3.1 Problemstellung 275
10.3.2 Konzept der initial ramdisk 276
10.3.3 Ablauf des Bootvorgangs mit initrd 276
10.3.4 Bootloader 277
10.3.5 Anwendung von initrd bei SUSE 278
10.3.6 Mögliche Schwierigkeit – Selbstkompilierte Kernel . 279
10.3.7 Ausblick 280
10.4 Das SUSE Rettungssystem 280
10.4.1 Das Rettungssystem starten 281
10.4.2 Das Rettungssystem benutzen 283
10.5 Virtuelle Konsolen 284
10.6 Tastaturbelegung 285
10.7 Lokale Anpassungen — I18N/L10N 286
10.7.1 Einige Beispiele 287
10.7.2 Anpassung für Sprachunterstützung 287

11 Das Bootkonzept **289**
11.1 Das init-Programm 290
11.2 Die Runlevels 291
11.3 Wechsel des Runlevels 292
11.4 Die Init-Skripten 293
11.4.1 Init-Skripten hinzufügen 296
11.5 Der YaST Runlevel-Editor 297
11.6 SuSEconfig und /etc/sysconfig 299
11.7 Der YaST Sysconfig-Editor 301

12 Das X Window System **305**
12.1 Installation des X Window Systems optimieren 306
12.1.1 Screen-Section 308
12.1.2 Device-Section 310
12.1.3 Monitor- und Modes-Section 311
12.2 Installation und Konfiguration von Fonts 312
12.2.1 Details zu Font-Systemen 313
12.3 Konfiguration von OpenGL/3D 318
12.3.1 Hardwareunterstützung 318
12.3.2 OpenGL-Treiber 319
12.3.3 Diagnose-Tool 3Ddiag 319
12.3.4 OpenGL-Testprogramme 320
12.3.5 Troubleshooting 320
12.3.6 Installationssupport 320
12.3.7 Weiterführende Online-Dokumentation 321

13 Druckerbetrieb **323**
13.1 Update, Upgrade und Migration 324
13.1.1 Aktualisierung von CUPS 324
13.1.2 Migration von LPRng/lpdfilter nach CUPS 325
13.2 Vorbereitungen und weitere Überlegungen 327
13.3 Druckeranbindung — Methoden und Protokolle 329
13.4 Installation der Software 330

13.5 Konfiguration des Druckers 331
13.5.1 Lokaler Drucker 331
13.5.2 Netzwerkdrucker 331
13.5.3 Konfigurationsarbeiten 333
13.6 Besonderheiten bei SUSE LINUX 334
13.6.1 Web-Frontend (CUPS) und KDE-Administration . . . 334
13.6.2 Änderungen beim cupsd 334
13.6.3 PPD-Dateien in SUSE Linux-Paketen 336
13.7 Mögliche Probleme und deren Lösung 339
13.7.1 Drucker ohne Standarddruckersprache 339
13.7.2 Geeignete PPD-Datei für PostScript-Drucker fehlt . . 339
13.7.3 Parallel-Ports 340
13.7.4 Druckeranschluss via Netzwerk 341
13.7.5 Fehlerhafte Ausdrucke ohne Fehlermeldung 344
13.7.6 Abgeschaltete Warteschlangen 344
13.7.7 Löschen von Druckaufträgen bei CUPS-Browsing . . 344
13.7.8 Druckaufträge fehlerhaft oder Datentransfer gestört . 345
13.7.9 Ursachen für Probleme im CUPS-Drucksystem . . . 346

14 Das Hotplug-System 347
14.1 Geräte und Schnittstellen 348
14.2 Hotplug Events 349
14.3 Hotplug Agenten 349
14.4 Automatisches Laden von Modulen 350
14.5 Netzwerkgeräte und Schnittstellenbezeichnungen 351
14.6 Hotplug mit PCI 351
14.7 Coldplug 352
14.8 Fehleranalyse 352
14.8.1 Protokoll-Dateien 352
14.8.2 Boot-Probleme 353
14.8.3 Der Event-Recorder 353

15 Dynamische Device Nodes mit udev **355**
15.1 Grundlagen zum Erstellen von Regeln 356
15.2 Automatisierung bei NAME und SYMLINK 357
15.3 Reguläre Ausdrücke in Schlüsseln 357
15.4 Tipps zur Auswahl geeigneter Schlüssel 358
15.5 Konsistente Namen für Massen-Speichergeräte 359

16 Mobiles Arbeiten unter Linux **361**
16.1 PCMCIA 362
16.1.1 Die Hardware 362
16.1.2 Die Software 362
16.1.3 Die Konfiguration 364
16.1.4 Wenn's trotzdem nicht geht 366
16.1.5 Installation via PCMCIA 371
16.1.6 Weitere Hilfsprogramme 372
16.1.7 Kernel oder PCMCIA Paket aktualisieren 372
16.1.8 Weiterführende Informationen 373
16.2 SCPM – System Configuration Profile Management 373
16.2.1 Grundbegriffe und Grundlagen 374
16.2.2 Der YaST Profil-Manager 375
16.2.3 SCPM einrichten 375
16.2.4 Profile anlegen und verwalten 376
16.2.5 Zwischen Konfigurationsprofilen umschalten 376
16.2.6 Erweiterte Profileinstellungen 377
16.2.7 Profilauswahl beim Booten 379
16.2.8 Probleme und deren Lösung 380
16.3 IrDA – Infrared Data Association 381
16.3.1 Software 382
16.3.2 Konfiguration 382
16.3.3 Verwendung 382
16.3.4 Troubleshooting 383
16.4 Bluetooth – Geräte drahtlos verbinden 384

16.4.1 Profile 384
16.4.2 Software 385
16.4.3 Konfiguration 385
16.4.4 Systemkomponenten und nützliche Hilfsmittel . . . 386
16.4.5 Beispiele 388
16.4.6 Troubleshooting 390
16.4.7 Weitere Informationen 391

17 Powermanagement **393**
17.1 Stromsparfunktionen 394
17.2 APM 396
17.2.1 Der APM-Daemon (apmd) 397
17.2.2 Weitere Befehle 399
17.3 ACPI 399
17.3.1 Praxis 400
17.3.2 Der ACPI-Daemon (acpid) 403
17.3.3 Weitere Tools 403
17.3.4 Mögliche Probleme und Lösungen 403
17.4 Pause für die Festplatte 405
17.5 Das powersave Paket 407
17.5.1 Konfiguration des powersave Pakets 407
17.5.2 Konfiguration von APM und ACPI 408
17.5.3 Zusätzliche ACPI-Features 410
17.5.4 Troubleshooting 411
17.6 Das YaST Powermanagement-Modul 413
17.7 WOL – Wake on Lan 416
17.7.1 BIOS-Konfiguration 417
17.7.2 Einrichtung mit YaST 418
17.7.3 Aufwecken von Rechnern 419
17.7.4 Weitere Informationen 419

18 Dateisysteme unter Linux **421**
18.1 Glossar . . . 422
18.2 Die wichtigsten Dateisysteme unter Linux . . . 422
18.2.1 Ext2 . . . 423
18.2.2 Ext3 . . . 424
18.2.3 ReiserFS . . . 426
18.2.4 JFS . . . 427
18.2.5 XFS . . . 427
18.3 Weitere unterstützte Dateisysteme . . . 429
18.4 Large File Support unter Linux . . . 430
18.5 Weitere Informationen . . . 431

19 Hochverfügbarkeit unter Linux **433**
19.1 Wichtige Begriffe . . . 434
19.2 Ein minimales Beispielszenario . . . 435
19.3 Komponenten einer Hochverfügbarkeitslösung . . . 436
19.4 Die Softwareseite von Hochverfügbarkeit . . . 438
19.4.1 heartbeat . . . 438
19.4.2 RAID . . . 438
19.4.3 rsync . . . 438
19.4.4 DRBD . . . 439
19.5 Clustering . . . 439
19.5.1 Cluster Alias . . . 439
19.5.2 Linux Virtual Server . . . 439
19.5.3 High-Availability Cluster . . . 440
19.6 Weitere Informationen . . . 440
19.6.1 Hochverfügbarkeit (HA) allgemein und heartbeat . . . 440
19.6.2 DRBD . . . 441
19.6.3 RAID . . . 441
19.6.4 Clustering . . . 441

20 PAM – Pluggable Authentication Modules **443**
20.1 Aufbau einer PAM-Konfigurationsdatei 444
20.2 Die PAM-Konfiguration von sshd 446
20.3 Konfiguration der PAM-Module 447
20.3.1 pam_unix2.conf 448
20.3.2 pam_env.conf 448
20.3.3 pam_pwcheck.conf 449
20.3.4 limits.conf 450
20.4 Weitere Informationen 450

III Dienste **451**

21 Grundlagen der Vernetzung **453**
21.1 TCP/IP – Das von Linux verwendete Protokoll 454
21.1.1 Schichtenmodell 455
21.1.2 IP-Adressen und Routing 458
21.1.3 Domain Name System – DNS 461
21.2 IPv6 – Internet der nächsten Generation 463
21.2.1 Vorteile von IPv6 464
21.2.2 Das Adresssystem von IPv6 465
21.2.3 IPv4 versus IPv6 – Wandern zwischen den Welten . . 470
21.2.4 Weiterführende Literatur und Links zu IPv6 471
21.3 Manuelle Netzwerkkonfiguration 472
21.3.1 Konfigurationsdateien 473
21.3.2 Startup-Skripten 480
21.4 Die Einbindung ins Netzwerk 481
21.4.1 Vorbereitungen 481
21.4.2 Netzwerkkarte konfigurieren mit YaST 482
21.4.3 S/390; zSeries: Netzwerkkonfiguration mit YaST . . . 485
21.4.4 Modem 486
21.4.5 DSL 489
21.4.6 ISDN 491

21.4.7 Hotplug/PCMCIA 496
21.4.8 Konfiguration von IPv6 496
21.5 Routing unter SuSE Linux 497
21.6 SLP — Dienste im Netz vermitteln 498
21.6.1 SLP-Unterstützung in SUSE LINUX 498
21.6.2 Weitere Informationen 501
21.7 DNS – Domain Name System 502
21.7.1 Nameserver BIND starten 502
21.7.2 Die Konfigurationsdatei /etc/named.conf 504
21.7.3 Konfigurationsoptionen im Abschnitt options 505
21.7.4 Der Konfigurationsabschnitt Logging 506
21.7.5 Aufbau der Zonen-Einträge 506
21.7.6 Aufbau der Zonendateien 508
21.7.7 Sichere Transaktionen 512
21.7.8 Zonendaten dynamisch aktualisieren 513
21.7.9 DNSSEC 513
21.7.10 Konfiguration mit YaST 514
21.7.11 Weitere Informationen 520
21.8 LDAP – Ein Verzeichnisdienst 521
21.8.1 LDAP versus NIS 524
21.8.2 Aufbau eines LDAP-Verzeichnisbaums 525
21.8.3 Serverkonfiguration mit slapd.conf 528
21.8.4 Handhabung von Daten im LDAP-Verzeichnis 533
21.8.5 LDAP-Server: Konfiguration mit YaST 537
21.8.6 Der YaST LDAP-Client 543
21.8.7 Weitere Informationen 551
21.9 NIS – Network Information Service 553
21.9.1 NIS Master und Slave Server 554
21.9.2 Das NIS-Client-Modul in YaST 556
21.10 NFS – verteilte Dateisysteme 557
21.10.1 Importieren von Dateisystemen mit YaST 558
21.10.2 Manuelles Importieren von Dateisystemen 558

21.10.3 Exportieren von Dateisystemen mit YaST 559
21.10.4 Manuelles Exportieren von Dateisystemen 560
21.11 DHCP 563
21.11.1 Das DHCP-Protokoll 563
21.11.2 DHCP-Softwarepakete 564
21.11.3 Der DHCP-Server dhcpd 564
21.11.4 Rechner mit fester IP-Adresse 566
21.11.5 Besonderheiten bei SUSE LINUX 568
21.11.6 DHCP-Konfiguration mit YaST 569
21.11.7 Weitere Informationen 576
21.12 Zeitsynchronisation mit xntp 577
21.12.1 Konfiguration im Netzwerk 578
21.12.2 Einrichten einer lokalen Zeitnormalen 579

22 Der Webserver Apache **581**
22.1 Grundlagen 582
22.1.1 Webserver 582
22.1.2 HTTP 582
22.1.3 URLs 582
22.1.4 Automatische Ausgabe einer Standardseite 583
22.2 HTTP-Server mit YaST einrichten 583
22.3 Apache Module 584
22.4 Neuerungen mit Apache 2 585
22.5 Threads 586
22.6 Installation 587
22.6.1 Paketauswahl in YaST 587
22.6.2 Apache aktivieren 587
22.6.3 Module für aktive Inhalte 587
22.6.4 Zusätzliche empfehlenswerte Pakete 588
22.6.5 Installation von Modulen mit apxs 588
22.7 Konfiguration 589
22.7.1 Konfiguration mit SuSEconfig 589

22.7.2 Manuelle Konfiguration 590
22.8 Apache im Einsatz 594
22.9 Aktive Inhalte 595
22.9.1 Server Side Includes: SSI 596
22.9.2 Common Gateway Interface: CGI 596
22.9.3 GET und POST 597
22.9.4 Sprachen für CGI 597
22.9.5 Aktive Inhalte mit Modulen erzeugen 598
22.9.6 mod_perl 598
22.9.7 mod_php4 600
22.9.8 mod_python 601
22.9.9 mod_ruby 601
22.10 Virtual Hosts 601
22.10.1 Namensbasierte Virtual Hosts 602
22.10.2 IP-basierte Virtual Hosts 603
22.10.3 Mehrere Instanzen von Apache 604
22.11 Sicherheit 605
22.11.1 Das Risiko gering halten 605
22.11.2 Zugriffsrechte 605
22.11.3 Immer auf dem Laufenden bleiben 606
22.12 Troubleshooting 606
22.13 Weitere Dokumentation 607
22.13.1 Apache 607
22.13.2 CGI 607
22.13.3 Sicherheit 608
22.13.4 Weitere Quellen 608

23 Datei-Synchronisation **609**
23.1 Software zur Datensynchronisation 610
23.1.1 unison 610
23.1.2 CVS 611
23.1.3 subversion 611
23.1.4 mailsync 612
23.1.5 rsync 612
23.2 Kriterien für die Programmauswahl 612
23.2.1 Client-Server-Modell versus Gleichberechtigung . . . 612
23.2.2 Portabilität 613
23.2.3 Interaktiv versus Automatisch 613
23.2.4 Konflikte: Auftreten und Lösung 613
23.2.5 Dateiwahl, Dateien hinzufügen 614
23.2.6 Geschichte 614
23.2.7 Datenmenge / Plattenbedarf 614
23.2.8 GUI 614
23.2.9 Anforderungen an den Benutzer 615
23.2.10 Sicherheit gegen Angriffe 615
23.2.11 Sicherheit gegen Datenverlust 615
23.3 Einführung unison 616
23.3.1 Einsatzgebiete 616
23.3.2 Voraussetzungen 616
23.3.3 Bedienung 617
23.3.4 Weiterführende Literatur 618
23.4 Einführung CVS 618
23.4.1 Einsatzgebiete 618
23.4.2 Einrichten eines CVS-Servers 619
23.4.3 Benutzung von CVS 619
23.4.4 Weiterführende Literatur 621
23.5 Einführung in subversion 622
23.5.1 Einsatzgebiete 622
23.5.2 Einrichten eines Subversion-Servers 622

23.5.3 Benutzung 623
23.5.4 Weiterführende Literatur 625
23.6 Einführung in rsync 625
23.6.1 Einsatzgebiet 625
23.6.2 Konfiguration und Benutzung 625
23.6.3 Mögliche Probleme 627
23.6.4 Weiterführende Literatur 627
23.7 Einführung mailsync 627
23.7.1 Einsatzgebiet 627
23.7.2 Konfiguration und Benutzung 628
23.7.3 Mögliche Probleme 630
23.7.4 Weiterführende Literatur 631

24 Heterogene Netzwerke **633**
24.1 Samba 634
24.1.1 Einführung in Samba 634
24.1.2 Installation und Konfiguration des Servers 636
24.1.3 Samba als Anmelde-Server 641
24.1.4 Installation und Konfiguration mit YaST 642
24.1.5 Installation der Clients 643
24.1.6 Optimierung 645
24.2 Netatalk 646
24.2.1 Konfiguration des Fileservers 648
24.2.2 Konfiguration des Druckservers 652
24.2.3 Starten des Servers 653
24.2.4 Weiterführende Informationen 653

25 Internet **655**
25.1 Der smpppd als Einwahlhelfer 656
25.1.1 Programmkomponenten zur Einwahl ins Internet . . 656
25.1.2 Die Konfiguration des smpppd 656
25.1.3 kinternet und cinternet im Remote-Einsatz 657
25.2 Konfiguration eines ADSL / T-DSL Anschlusses 658

25.2.1 Standardkonfiguration 658
25.2.2 DSL Verbindung per Dial-on-Demand 659
25.3 Proxy-Server: Squid 659
25.3.1 Was ist ein Proxy-Cache? 660
25.3.2 Informationen zu Proxy-Cache 660
25.3.3 Systemanforderungen 662
25.3.4 Squid starten 664
25.3.5 Die Konfigurationsdatei /etc/squid/squid.conf . . . 666
25.3.6 Konfiguration eines Transparenten Proxy 671
25.3.7 cachemgr.cgi 674
25.3.8 squidGuard 676
25.3.9 Erzeugen von Cache-Berichten mit Calamaris 678
25.3.10 Weitere Informationen zu Squid 678

26 Sicherheit im Netzwerk 679
26.1 X.509-Zertifizierung mit YaST 680
26.1.1 Grundlagen der digitalen Zertifizierung 680
26.1.2 YaST-Module für CA-Management 684
26.2 VPN mit SUSE LINUX 694
26.2.1 Road Warrior Server einrichten 695
26.2.2 VPN-Linux-Client mit FreeS/WAN einrichten 698
26.2.3 IPsec-Clients auf Windows XP und Windows 2000 . . 701
26.3 Masquerading und Firewall 705
26.3.1 Paketfilterung mit iptables 705
26.3.2 Grundlagen des Masquerading 708
26.3.3 Grundlagen Firewalling 709
26.3.4 SuSEfirewall2 710
26.3.5 Weitere Informationen 714
26.4 SSH – secure shell, die sichere Alternative 715
26.4.1 Das OpenSSH-Paket 715
26.4.2 Das ssh-Programm 716
26.4.3 scp – sicheres Kopieren 716

26.4.4 sftp - sicherere Dateiübertragung 717
26.4.5 Der SSH Daemon (sshd) – die Serverseite 717
26.4.6 SSH-Authentifizierungsmechanismen 719
26.4.7 X-, Authentifizierungs- und sonstige Weiterleitung . 720
26.5 Netzwerkauthentifizierung — Kerberos 721
26.5.1 Kerberos-Terminologie 722
26.5.2 Wie funktioniert es? 724
26.5.3 Auswirkungen von Kerberos für den Benutzer 727
26.5.4 Weitere Informationen über Kerberos 728
26.6 Installation und Administration von Kerberos 729
26.6.1 Festlegung der Kerberos-Realms 729
26.6.2 Einrichtung der KDC-Hardware 730
26.6.3 Zeitsynchronisation 731
26.6.4 Konfiguration der Protokollfunktion 732
26.6.5 Installation des KDC 732
26.6.6 Konfiguration von Kerberos-Clients 735
26.6.7 Einrichtung der Fernadministration 739
26.6.8 Erstellung von Kerberos Host Principals 741
26.6.9 Aktivierung der PAM-Unterstützung für Kerberos . 743
26.6.10 SSH mit Kerberos-Authentifizierung 743
26.6.11 Benutzung von LDAP und Kerberos 745
26.7 Sicherheit ist Vertrauenssache 748
26.7.1 Grundlagen 748
26.7.2 Lokale Sicherheit und Netzwerksicherheit 748
26.7.3 Tipps und Tricks: Allgemeine Hinweise 758
26.7.4 Zentrale Meldung neuer Sicherheitsproblemen 760

IV Administration **763**

27 Access Control Lists unter Linux **765**
27.1 Warum ACLs? . . . 766
27.2 Definitionen . . . 767
27.3 Umgang mit ACLs . . . 768
27.3.1 Aufbau von ACL-Einträgen . . . 768
27.3.2 ACL-Einträge und Berechtigungsbits . . . 769
27.3.3 Ein Verzeichnis mit Access ACL . . . 770
27.3.4 Ein Verzeichnis mit Default ACL . . . 774
27.3.5 Auswertung einer ACL . . . 777
27.4 Unterstützung in Anwendungen . . . 777

28 Utilities zur Systemüberwachung **779**
28.1 Konventionen . . . 780
28.2 Liste der geöffneten Dateien: lsof . . . 780
28.3 Wer greift auf Dateien zu: fuser . . . 781
28.4 Eigenschaften einer Datei: stat . . . 782
28.5 Prozesse: top . . . 782
28.6 Prozessliste: ps . . . 783
28.7 Prozessbaum: pstree . . . 784
28.8 Wer macht was: w . . . 785
28.9 Speichernutzung: free . . . 785
28.10 Kernel Ring Buffer: dmesg . . . 786
28.11 Dateisysteme: mount, df und du . . . 787
28.12 Das /proc Dateisystem . . . 788
28.13 procinfo . . . 790
28.14 PCI Resourcen: lspci . . . 791
28.15 System Calls eines Programmlaufes: strace . . . 792
28.16 Library Calls eines Programmlaufes: ltrace . . . 793
28.17 Welche Library wird benötigt: ldd . . . 794
28.18 Interprozess-Kommunikation: ipcs . . . 794

V Anhang **795**

A Informationsquellen und Dokumentationen **797**

B Manual-Page von e2fsck **801**

C Manual-Page von reiserfsck **807**

D Deutsche Übersetzung der GNU General Public License **813**

Literaturverzeichnis **825**

Vorwort

Über dieses Buch

Dieses Buch begleitet Sie von der Erstinstallation Ihres SUSE LINUX Enterprise Server bis hin zur umfassenden Systemkonfiguration und komplexen Administrationsaufgaben. Sie finden die Installations- und Administrationsbeschreibungen für alle von SUSE LINUX Enterprise Server unterstützten Hardwareplattformen komprimiert in diesem Handbuch.

Hinweis

Informationen zur Installationsvorbereitung

Detaillierte Informationen zur Vorbereitung Ihrer Hardware-Plattform finden Sie im Handbuch *Architekturspezifika*, das sich unter dem Namen `preparation.pdf` im Verzeichnis `/docu/` auf der ersten CD des SUSE LINUX Enterprise Server befindet.

Hinweis

Aufbau

Dieses Handbuch gliedert sich in vier Themenkomplexe

Installation Dieser Teil des Buches begleitet Sie vom ersten Installationsdialog bis zum fertig konfigurierten System. Sie erfahren ausserdem, wie Sie die verschiedenen Installationstypen von SUSE LINUX Enterprise Server einsetzen, Installationsquellen konfigurieren und wie Sie einzelne Softwarepakete oder auch das gesamte Betriebssystem aktualisieren.

System In diesem Teil des Buches erfahren Sie Details zum Aufbau und der Funktionsweise Ihres Linux-Systems, zur Unterscheidung von 32-(31-)bit und 64-bit Welt sowie zur Einrichtung einer grafischen Oberfläche und einer Druckinfrastruktur.

Dienste Dieser Teil des Buches behandelt die wesentlichen Serverdienste auf Ihrem System sowie deren Konfiguration mit YaST. Abschließend runden Informationen zum Thema Sicherheit, zu Firewalls, CA-Verwaltung, VPN-Konfiguration und Authentifizierungsverfahren diesen Teil ab.

Administration Hier finden Sie Informationen über den Einsatz von Dateisystem-ACLs und ein Kapitel über die verschiedenen System-Monitoring Programme unter Linux.

Im Anhang finden Sie eine Übersicht über die wichtigsten Informationsquellen zu Linux.

Wie dieses Buch zu lesen ist

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

Auszeichnung	Bedeutung
YaST	die Angabe eines Programmnamens
`/etc/passwd`	die Angabe einer Datei oder eines Verzeichnisses
⟨*platzhalter*⟩	die Zeichenfolge `platzhalter` (inkl. Winkelklammern) ist durch den tatsächlichen Wert zu ersetzen
`PATH`	eine Umgebungsvariable mit dem Namen `PATH`
`192.168.1.2`	der Wert einer Variable
`ls`	die Angabe eines einzugebenden Befehls
`user`	die Angabe eines Benutzers
Alt	eine zu drückende Taste

Strg+Alt+Entf	gleichzeitig zu drückende Tasten
"Permission denied"	Meldungen des Systems
‘System updaten’	Menü-Punkte, Buttons

Neben den typografischen Konventionen verwendet dieses Buch folgende Namenskonventionen und Abkürzungen im Zusammenhang mit den von SUSE LINUX Enterprise Server unterstützten Hardwarearchitekturen:

Abkürzung	**Voller Name/Prozessorbezeichnung**
x86	x86
AMD64	AMD64
EM64T	Intel EM64T
IPF	Intel Itanium Processor Family
POWER	IBM POWER
S/390	IBM S/390
zSeries	IBM zSeries

Um im Fließtext Differenzen zwischen den einzelnen Plattformen zu kennzeichnen, verwenden die Autoren die im Folgenden aufgelisteten Konventionen. Die Art der Kennzeichnung ist von der Menge der divergierenden Information abhängig. Zum besseren Verständnis hier kurze Beispiele:

Unterscheiden sich innerhalb eines Satzes oder Abschnittes nur wenige Worte oder Zeichen, wird die Unterscheidung ohne weitere Kennzeichnung in den Fließtext eingearbeitet.

Hinweis

zSeries: Ein kurzer Tipp

Kurze Tipps, Hinweise oder Warnungen, die exklusiv auf eine oder mehrere Architekturen zutreffen, werden durch das Plattformkürzel gefolgt vom eigentlichen Titel des Hinweises gekennzeichnet.

Hinweis

► **EM64T**
Ganze Absätze, die sich zwischen den Plafformen unterscheiden, werden durch zwei grafische Symbole (schwarze Dreiecke) und das Plattformkürzel getrennt. ◄

AMD64: Ein Abschnitt allein für AMD64

Befasst sich ein kompletter Abschnitt eines Kapitels mit einer Plattform, wird dies ähnlich wie bei Tipps, Hinweisen und Warnungen durch das Plattformkürzel im Titel eingeleitet, damit bereits das Inhaltsverzeichnis dieses Buches diese Unterscheidung wiederspiegelt.

Die Kennzeichnung von Screenshots oder Codebeispielen erfolgt analog über die Einleitung der jeweiligen Bildunterschrift oder der Beispielüberschrift durch das Plattformkürzel. Wird kein Kürzel verwendet, ist die Information allgemein gültig.

Zielgruppe

Die Autoren setzen bei den Lesern dieses Buches folgendes Grundwissen voraus:

- Sie kennen sich in der Terminologie Ihre Hardwareplattform betreffend aus oder haben Zugang zu entsprechender Dokumentation des Hardwareherstellers.
- Sie sind mit den Eigenschaften und Besonderheiten Ihrer Hardwareplattform vertraut.
- Sie verfügen mindestens über Grundwissen die Adminstration eines Linux-System betreffend.

Teil I

Installation

Installation mit YaST

Ihre Hardware ist — wie im Handbuch *Architekturspezifika* beschrieben — auf die Installation von SUSE LINUX Enterprise Server vorbereitet. Nachdem Verbindung zum Installationssystem hergestellt ist übernimmt der SUSE Systemassistent YaST die Kontrolle. Er wird Sie durch die gesamte Installation und Konfiguration des Systems begleiten.

1.1 S/390, zSeries: Systemstart zur Installation 8
1.2 Systemstart zur Installation 8
1.3 Startbildschirm 10
1.4 Sprachauswahl 13
1.5 S/390, zSeries: Konfiguration der Festplatten . . . 14
1.6 Installationsmodus 15
1.7 Installationsvorschlag 16
1.8 Installation abschließen 39
1.9 Hardware-Konfiguration 48
1.10 Grafisches Login 50

1.1 S/390, zSeries: Systemstart zur Installation

Für die S/390 und zSeries Plattformen von IBM wird der Systemstart (IPL) für die Installation wie im Handbuch *Architekturspezifika* beschrieben initiiert. SUSE LINUX Enterprise Server für diese Plattformen hat keinen Splashscreen, da Kernel und initrd für die Installation vom Benutzer manuell geladen werden. Sobald die Verbindung zum Installationssystem über VNC, X oder SSH hergestellt ist, startet YaST zur Installation. Die Übergabe von Kernel- oder Bootparametern geschieht über ein parmfile (wie in Kapitel *Das parmfile: Automatisierte Systemkonfiguration* im Handbuch *Architekturspezifika* beschrieben).

Hinweis

S/390, zSeries: Weitere Schritte

Lesen Sie beginnend mit Abschnitt 1.4 auf Seite 13 die Beschreibung des Installationsvorgangs mit YaST nach.

Hinweis

1.2 Systemstart zur Installation

Legen Sie das Installationsmedium von SUSE LINUX in das Laufwerk und starten Sie den Rechner neu. Das SUSE LINUX Installationsprogramm wird dann geladen und die Installation beginnt.

1.2.1 Mögliche Probleme beim Systemstart

Sollte Ihr Rechner nicht vom Installationsmedium booten, so kann das verschiedene Ursachen haben:

- Die Start-Reihenfolge des Rechners ist im BIOS (engl. *Basic Input Output System*) nicht richtig eingestellt. Informationen zum Ändern der Einstellungen im BIOS erhalten Sie in der Dokumentation Ihres Mainboards bzw. in den folgenden Abschnitten.

  Das BIOS ist ein Stück Software, mit der die Grundfunktionalität des Computers gestartet wird. Die Hersteller von Mainboards stellen ein speziell auf die Hardware angepasstes BIOS zur Verfügung.

Der Aufruf des BIOS-Setups kann erst zu einem bestimmten Zeitpunkt erfolgen: Beim Neustart des Rechners wird eine Diagnose der Hardware durchgeführt, so wird u. a. der Arbeitsspeicher getestet. Sie können dies beim Hochzählen des Systemspeichers verfolgen. Zur gleichen Zeit wird darunter oder am unteren Bildschirmrand angezeigt, mit welcher Taste Sie das BIOS-Setup aufrufen können. Üblicherweise müssen dazu die Tasten (Del), (F1) oder (Esc) gedrückt werden. Statt (Del) wird die Taste mitunter auch (Entf) genannt. Drücken Sie die entsprechende Taste, um das BIOS-Setup zu starten.

Ändern Sie die Bootsequenz wie folgt: Bei einem AWARD-BIOS suchen Sie den Eintrag 'BIOS FEATURES SETUP'. Andere Hersteller verwenden ähnliche Einträge wie zum Beispiel 'ADVANCED CMOS SETUP'. Wählen Sie den entsprechenden Eintrag aus und bestätigen Sie mit (Return).

Die Startreihenfolge kann beim Unterpunkt 'BOOT SEQUENCE' eingestellt werden. Die Voreinstellung ist oftmals 'C, A' oder 'A, C'. Im ersten Fall sucht der Rechner beim Booten das Betriebssystem zuerst auf der Festplatte (C) und dann im Diskettenlaufwerk (A). Drücken Sie dann solange die Taste (Bild auf) bzw. (Bild ab), bis die Sequenz 'A,CDROM,C' angezeigt wird.

Verlassen Sie die Einstellungen durch Drücken von (Esc). Um die Änderungen zu speichern, wählen Sie 'SAVE & EXIT SETUP' oder drücken Sie (F10). Bestätigen Sie dann Ihre Einstellungen mit (Y).

Hinweis

Tastaturbelegung im BIOS

Häufig bietet das BIOS keine deutsche Tastaturbelegung an, sondern nur die amerikanische: Die Tasten (Y) und (Z) sind vertauscht.

Hinweis

Haben Sie ein SCSI-CD-ROM-Laufwerk, müssen Sie zum Beispiel bei einem Adaptec Hostadapter mit (Strg)-(A) dessen BIOS aufrufen. Nach der Auswahl von 'Disk Utilities' zeigt das System die angeschlossene Hardware an. Notieren Sie die SCSI-ID für Ihr CD-ROM. Das Menü verlassen Sie mit (Esc), um anschließend 'Configure Adapter Settings' zu öffnen. Unter 'Additional Options' finden Sie 'Boot Device Options'. Wählen Sie dieses Menü aus und drücken Sie (Return). Geben Sie nun die zuvor notierte ID des CD-ROM-Laufwerks ein und drücken Sie wieder (Return). Durch zweimaliges Drücken von (Esc) kehren Sie

zum Startbildschirm des SCSI-BIOS zurück, den Sie nach der Bestätigung mit ‘Yes’ verlassen, um den Rechner neu zu booten.

- Ihr CD-ROM-Laufwerk wird nicht unterstützt, weil es sich um ein älteres Laufwerk handelt.

1.3 Startbildschirm

Der Startbildschirm zeigt mehrere Auswahlmöglichkeiten für den weiteren Verlauf der Installation. Ganz oben befindet sich die Option ‘Boot from Harddisk’, die das bereits installierte System bootet. Weil nach erfolgreicher Installation die CD häufig zum Nachinstallieren von Software eingelegt wird, ist diese Option vorgewählt. Für die Installation wählen Sie aber bitte ‘Installation’ mit den Pfeil-Tasten aus. Danach wird YaST geladen und die Installation beginnt.

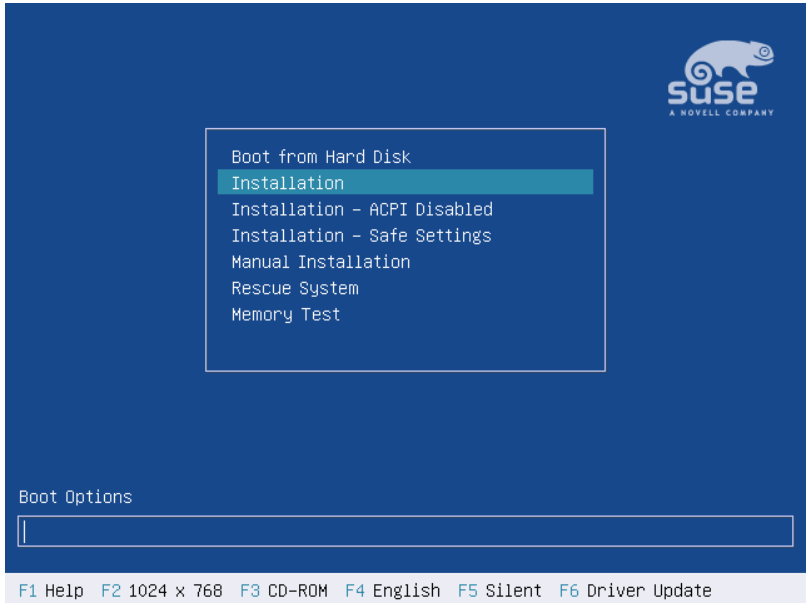

Abbildung 1.1: *Der Startbildschirm*

Die einzelnen Optionen im Startbildschirm bewirken folgendes:

Boot from Harddisk Bootet Ihr System von der Festplatte (jenes, das normalerweise beim Rechnerstart hochfährt). Diese Option ist vorgewählt.

Installation Die normale Installation, in der alle modernen Hardware-Funktionen aktiviert werden.

Installation - ACPI Disabled Wenn die normale Installation fehlschlägt, liegt dies möglicherweise daran, dass die System-Hardware mit der Unterstützung von ACPI *Advanced Configuration and Power Interface* nicht zurecht kommt. Mit dieser Option können Sie in solchen Fällen ohne ACPI-Unterstützung installieren.

Installation - Safe Settings Die DMA-Funktion (für das CD-ROM-Laufwerk) und problematisches Powermanagement werden deaktiviert. Experten können zusätzlich Kernel-Parameter in der Eingabezeile mitgeben oder verändern.

Manual Installation Wenn bestimmte Treiber, die beim Start der Installation automatisch geladen werden, Probleme bereiten, können Sie hier manuell installieren, das heisst diese Treiber werden dann nicht automatisch geladen. Dies funktioniert allerdings nicht, wenn Sie an Ihrem Rechner eine USB-Tastatur benutzen.

Rescue System Falls Sie keinen Zugriff mehr auf Ihr installiertes Linux-System haben, starten Sie den Rechner mit dem eingelegten Installationsmedium neu und wählen Sie diesen Punkt. Es startet dann ein Rettungssystem, ein minimales Linux-System ohne grafische Oberfläche, mit dem Experten Zugriff auf die Festplatten haben und eventuelle Fehler des installierten Systems reparieren können. Wenn Sie sich mit SUSE LINUX noch nicht so gut auskennen, können Sie alternativ die YaST-Systemreparatur verwenden. Details hierzu finden Sie im Kapitel 6 auf Seite 203

Memory Test (nur x86-Plattform) Testet den Arbeitsspeicher Ihres Systems durch wiederholtes Beschreiben und Auslesen. Der Test läuft endlos, weil Speicherfehler oft sehr sporadisch auftreten und nur bei sehr vielen Schreib-Lese-Zyklen entdeckt werden können. Wenn Sie den Verdacht haben, dass der Arbeitsspeicher defekt sein könnte, lassen Sie diesen Test einige Stunden laufen; falls nach einiger Zeit keine Fehler gemeldet werden, können Sie davon ausgehen, dass der Speicher intakt ist. Der Test wird durch Neustart des Rechners beendet.

Entsprechend der Funktionstastenleiste am unteren Bildschimrand können Sie mttels der angebenen F-Tasten verschieden Einstellungen für die Installation vornehmen.

(F1) Hier erhalten Sie eine kontextsensitive Hilfe zum jeweils aktiven Element des Startbildschirms.

(F2) Auswählen verschiedener Grafik-Modi für die Installation. Sollten bei der grafischen Installation Probleme auftreten, kann hier auch der Text-Modus ausgewählt werden.

(F3) Auswählen verschiedener Installationsquellen. Normalerweise wird vom eingelegten Installationsmedium installiert. Hier können Sie jedoch auch andere Quellen wie zum Beispiel FTP und NFS auswählen. Besondere Erwähnung verdient hier *SLP* (Service Location Protocol). Bei Installation in einem Netzwerk mit SLP-Server können mit dieser Option vor der eigentlichen Installation die auf dem Server verfügbaren Installationsquellen ausgewählt werden. Weitere Informationen zu *SLP* finden Sie im Abschnitt 21.6 auf Seite 498 .

(F4) Hier können Sie die Sprache für die Oberfläche des Startbildschirms einstellen.

(F5) Normalerweise sehen Sie beim Systemstart keine Fortschrittsmeldungen des Linux-Kernels, sondern einen Fortschrittsbalken. Wenn Sie diese Meldungen sehen wollen, wählen Sie hier bitte 'Native', für noch mehr zusätzliche Ausgaben 'Verbose'.

(F6) Wenn Sie für SUSE LINUX eine Treiber-Update-Diskette erhalten haben, können Sie diese hier zur Anwendung bringen. Sie werden dann im Lauf der Installation aufgefordert, das Update-Medium einzulegen.

Bei der Installation lädt SUSE LINUX einige Sekunden nach dem Startbildschirm ein minimales Linux-System, das den weiteren Installationsvorgang kontrolliert. Wenn sie den Ausgabemode auf auf 'Native' oder 'Verbose' umgestellt haben, sehen Sie jetzt auf dem Bildschirm zahlreiche Meldungen und Copyright-Hinweise. Zum Abschluss des Ladevorgangs wird das Installationsprogramm YaST gestartet und nach wenigen Sekunden sehen Sie die grafische Oberfläche, die Sie durch die Installation führen wird.

Jetzt beginnt die eigentliche Installation von SUSE LINUX mit dem Installationsprogramm YaST. Alle Bildschirmansichten von YaST folgen einem einheitlichen Schema. Sämtliche Eingabefelder, Auswahllisten und Buttons

der YaST-Bildschirme können Sie mit der Maus oder der Tastatur steuern. Bewegt sich der Cursor nicht, wurde Ihre Maus nicht automatisch erkannt. Verwenden Sie in diesem Fall bitte vorerst die Tastatur.

1.4 Sprachauswahl

SUSE LINUX und YaST stellen sich auf die von Ihnen gewünschte Sprache ein. Die Spracheinstellung, die Sie hier vornehmen, wird auch für das Tastaturlayout übernommen. Außerdem stellt YaST jetzt eine Standardzeitzone ein, die für Ihre Spracheinstellung am wahrscheinlichsten ist. Falls wider Erwarten die Maus noch nicht funktioniert, wählen Sie bitte mit den Pfeil-Tasten die gewünschte Sprache und drücken Sie dann so oft die Tab-Taste, bis der Button 'Übernehmen' aktiviert ist. Mit Return wird die Auswahl schließlich übernommen.

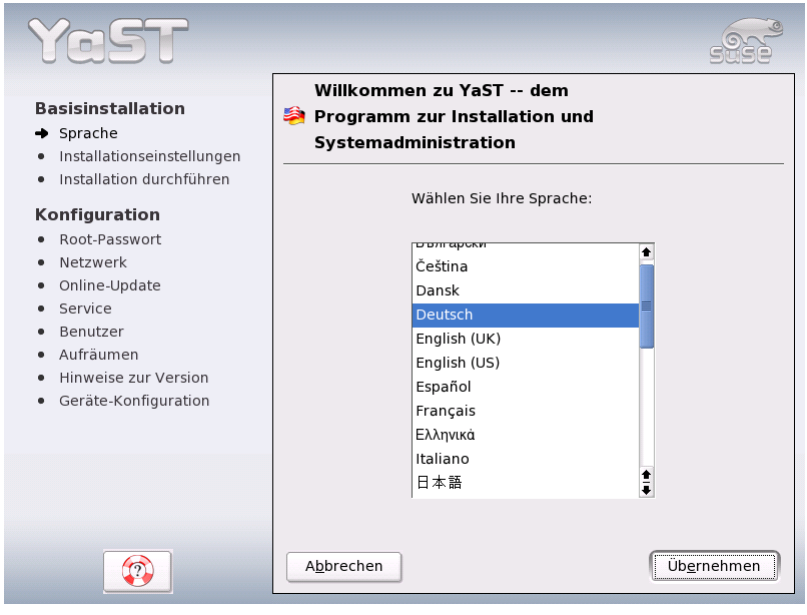

Abbildung 1.2: *Auswählen der Sprache*

1.5 S/390, zSeries: Konfiguration der Festplatten

Nach der Sprachauswahl öffnet sich bei der Installation von SUSE LINUX Enterprise Server auf IBM S/390 und zSeries der Dialog zur Konfiguration der angeschlossenen Festplatten. Sie haben die Möglichkeit, DASDs und Fibre Channel Attached SCSI Disks (ZFCP) zur Installation von SUSE LINUX Enterprise Server auszuwählen.

Wählen Sie 'DASD-Platten konfigurieren', öffnet sich ein Übersichtsdialog, der die im System vorhandenen DASDs listet. Um die Liste der angezeigten DASDs übersichtlicher zu gestalten, können Sie über die Eingabefelder oberhalb der Liste einen Kanalbereich festlegen, der angezeigt werden soll. Mit 'Filtern' wird die Filterung aktiviert (siehe Abb. 1.3).

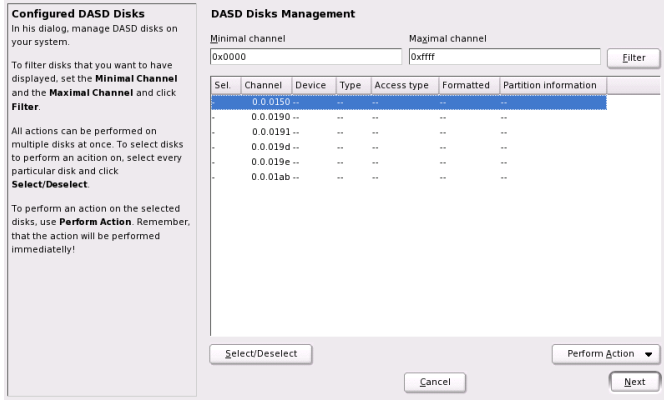

Abbildung 1.3: *S/390, zSeries: Auswählen eines DASD*

Im nächsten Schritt selektieren Sie die für die Installation verfügbaren DASDs. Selektieren Sie in der Liste die entsprechenden Einträge und klicken Sie auf 'Selektieren oder deselektieren'. Anschließend werden die selektierten DASDs aktiviert und für die Installation freigegeben. Klicken Sie auf 'Aktion durchführen' → 'Aktivieren' (siehe Abb. 1.4 auf der nächsten Seite). Die Formatierung der ausgewählten DASDs können Sie über 'Aktion durchführen' → 'Formatieren' jetzt vornehmen oder zu einem späteren Zeitpunkt mit dem YaST Partitionierer (siehe Abschnitt 1.7.4 auf Seite 22).

Möchten Sie der SUSE LINUX Enterprise Server Installation ZFCP-Platten

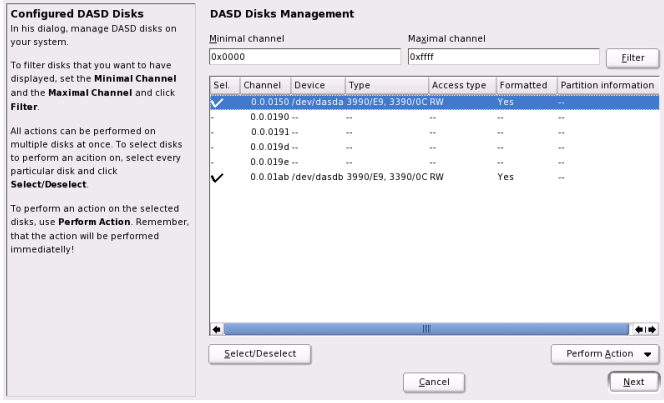

Abbildung 1.4: *S/390, zSeries: Aktivieren eines DASD*

zur Verfügung stellen, klicken Sie im Auswahldialog auf 'ZCFP-Platten konfigurieren'. Im dann folgenden Übersichtsdialog über die im System vorhandenen ZFCP-Platten, klicken Sie auf 'Hinzufügen', um in den Eingabedialog für die ZFCP-Parameter zu gelangen (siehe Abb. 1.5 auf der nächsten Seite).

Um eine neue ZFCP-Platte für die Installation zur Verfügung zu stellen, tragen Sie in den vorgesehenen Eingabefeldern 'Kanalnummer', 'WWPN' (World Wide Port) und 'FCP-LUN' ein, die die neue Platte eindeutig kennzeichnen (siehe Abbildung 1.6 auf Seite 17).

Verlassen Sie den nachfolgenden ZFCP-Übersichtsdialog mit 'Weiter' und den Plattenkonfigurationsdialog mit 'Beenden', um mit der Installation fortzufahren.

1.6 Installationsmodus

Dieser Dialog dient hauptsächlich dazu, zu entscheiden, ob Sie eine 'Neuinstallation' oder ein 'Update des bestehenden Systems' durchführen wollen. Letzteres geht natürlich nur, wenn bereits ein SUSE LINUX installiert ist. In diesem Fall können Sie dieses System mit 'Installiertes System starten' auch booten. Falls ihr bereits installiertes System einmal nicht mehr starten sollte, zum Beispiel weil versehentlich wichtige System-Konfigurationen zerstört wurden, können Sie mit 'Reparatur des instal-

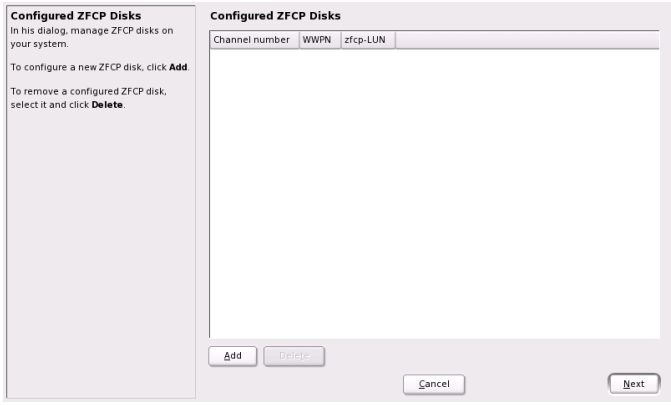

Abbildung 1.5: *S/390, zSeries: Überblick verfügbarer ZFCP-Platten*

lierten Systems' versuchen, das System wieder startbar zu machen. Falls bisher noch kein SUSE LINUX installiert ist, können Sie natürlich nur die Neuinstallation durchführen.

In den folgenden Abschnitten wird die Neuinstallation beschrieben. Weitere Informationen zum System-Update finden Sie im Kapitel 2.3.5 auf Seite 68. Eine Beschreibung der Möglichkeiten zur System-Reparatur finden Sie im Kapitel 6 auf Seite 203.

Klicken Sie bitte auf 'OK', um fortzufahren (Abb. 1.7 auf Seite 18).

1.7 Installationsvorschlag

Nach der Hardware-Erkennung erhalten Sie im orschlags-Dialog (siehe Abb. 1.8 auf Seite 19) Informationen zur erkannten Hardware und Vorschläge zur Installation und zur Partitionierung. Wenn Sie eine der Optionen anklicken und dann konfigurieren, kehren Sie anschließend mit den jeweils geänderten Werten immer wieder in diesen Vorschlags-Dialog zurück. Im Folgenden werden die einzelnen Installations-Einstellungen beschrieben.

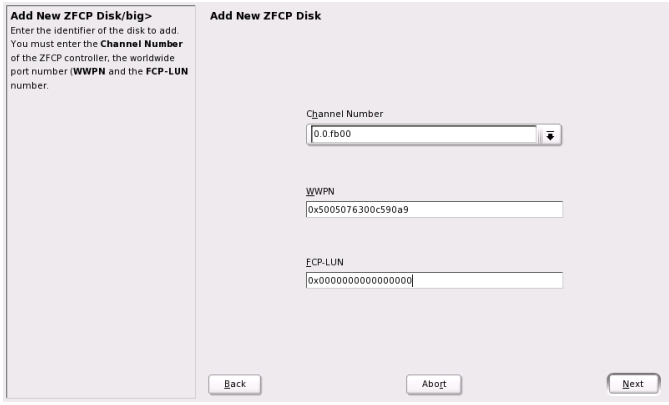

Abbildung 1.6: *S/390, zSeries: Neue ZFCP-Platte hinzufügen*

1.7.1 Installationsmodus

Hier können Sie nachträglich den gewählten Installationsmodus ändern. Die Möglichkeiten sind die gleichen, wie schon im Abschnitt 1.6 auf Seite 15 beschrieben.

1.7.2 Tastaturlayout

Hinweis

S/390, zSeries: Tastatur- und Mauskonfiguration

Die Installation auf IBM S/390 und zSeries erfolgt über ein entferntes Terminal. Am eigentlichen System ist keine lokale Maus oder Tastatur vorhanden.

Hinweis

Wählen Sie in diesem Dialog das gewünschte Tastaturlayout aus. In der Regel entspricht es der gewählten Sprache. Drücken Sie anschließend im Testfeld zum Beispiel die Tasten Ü oder Ä, um zu prüfen, ob die Umlaute richtig erscheinen. Mit 'Weiter' gelangen Sie wieder zu den Vorschlägen zurück.

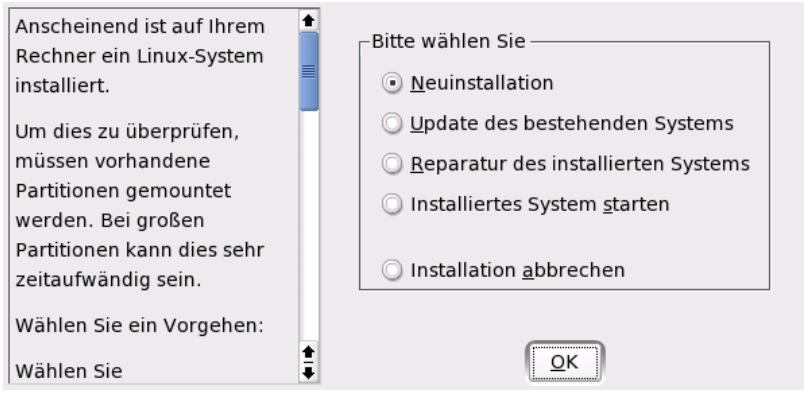

Abbildung 1.7: *Auswählen der Installationsart*

1.7.3 Maus

Sollte YaST die Maus nicht automatisch erkannt haben, drücken Sie bitte im Vorschlags-Dialog so oft die Tab-Taste, bis die Option 'Maus' markiert ist. Über die Leer-Taste erhalten Sie den in Abbildung 1.9 auf der nächsten Seite gezeigten Dialog zum Auswählen des Maustyps.

Verwenden Sie zur Auswahl der Maus die Tasten ↑ und ↓. Falls Sie eine Dokumentation zu Ihrer Maus besitzen, finden Sie dort eine Beschreibung des Maustyps. Bei ausgewählter Maus können Sie mit der Tastenkombination Alt-T die Maus testen, ohne sie dauerhaft auszuwählen. Falls die Maus nicht wie gewünscht reagiert, können Sie mit der Tastatur einen anderen Typ wählen und erneut testen. Mit Tab und Return wählen Sie die aktuelle Maus dauerhaft aus.

1.7.4 Partitionierung

In den meisten Fällen ist der Partitionierungsvorschlag von YaST sehr sinnvoll und kann ohne Änderungen übernommen werden. Wenn Sie jedoch besondere Vorstellungen hinsichtlich der Festplattenaufteilung haben, können Sie diese ebenfalls realisieren. Im Folgenden wird beschrieben, wie Sie dabei vorgehen können.

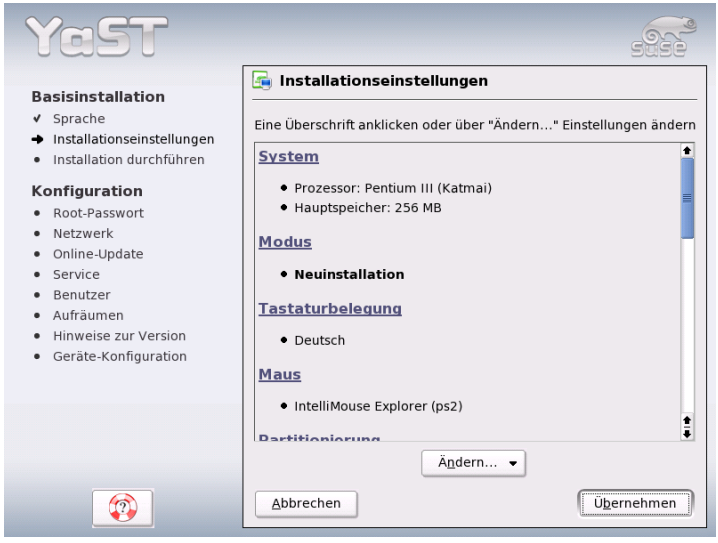

Abbildung 1.8: *Vorschlags-Dialog*

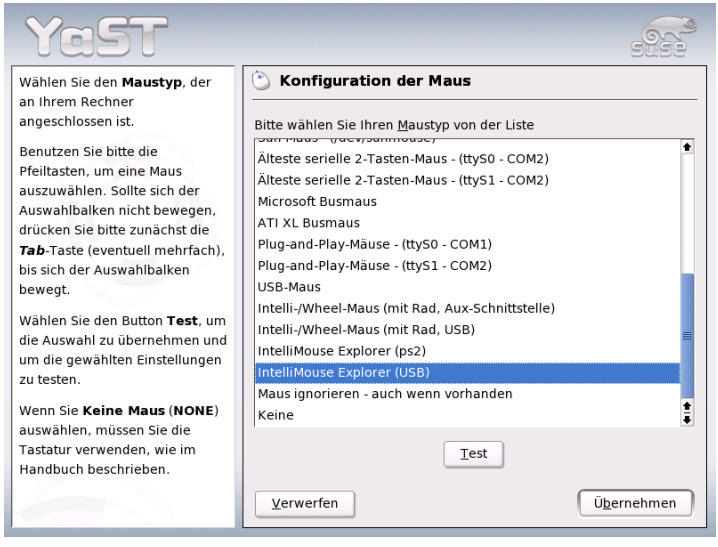

Abbildung 1.9: *Auswählen des Maustyps*

Partitionstypen

Hinweis

S/390, zSeries: „Festplatten“ unter IBM S/390 und zSeries

Unter SUSE LINUX Enterprise Server für IBM S/390 und zSeries werden SCSI-Festplatten und DASDs (*Direct Access Storage Device*) unterstützt. SCSI-Platten können wie nachfolgend beschrieben partitioniert werden. Für DASDs sind bis zu drei Partitionseinträge in der Partitionstabelle möglich.

Hinweis

Jede Festplatte enthält eine Partitionstabelle, die Platz für vier Einträge hat. Jeder Eintrag in der Partitionstabelle kann entweder für eine primäre Partition oder für eine erweiterte Partition stehen, wobei maximal *eine* erweiterte Partition möglich ist.

Primäre Partitionen haben einen einfachen Aufbau: Sie sind ein durchgehender Bereich von Plattenzylindern (physische Bereiche auf der Platte), der einem Betriebssystem zugeordnet ist. Mit primären Partitionen könnte man pro Festplatte maximal vier Partitionen einrichten; mehr passt nicht in die Partitionstabelle.

Werden mehr Partitionen benötigt, muss eine erweiterte Partition angelegt werden. Die erweiterte Partition ist ebenfalls ein durchgehender Bereich von Plattenzylindern. Sie kann aber weiter in so genannte *logische Partitionen* unterteilt werden, die selbst keinen Eintrag in der Partitionstabelle belegen. Die erweiterte Partition ist sozusagen ein Container, der die logischen Partitionen enthält.

Wenn Sie mehr als vier Partitionen benötigen, müssen Sie also beim Partitionieren nur darauf achten, dass Sie spätestens die vierte Partition als erweiterte Partition vorsehen und ihr den gesamten freien Zylinderbereich zuordnen. Darin können Sie dann beliebig viele logische Partitionen einrichten (das Maximum liegt bei 15 Partitionen für SCSI-Platten und bei 63 Partitionen für (E)IDE-Platten).

Für die Installation von SUSE LINUX sind beide Arten von Partitionen (primär und logisch) gleich gut geeignet.

Hinweise zum Speicherplatz

Wenn Sie YaST die Partitionierung der Festplatte überlassen, müssen Sie sich um den Speicherplatzbedarf und die Aufteilung der Festplatte (fast) keine Gedanken machen. Für den Fall, dass Sie aber selbst partitionieren

wollen, folgen hier einige Hinweise zu den Platzanforderungen der verschiedenen System-Typen.

Minimales System: 500 MB Dieses System hat keine grafische Oberfläche (X11), das heisst Sie können nur auf der Konsole arbeiten. Außerdem kann nur die elementarste Software installiert werden.

Minimales System mit grafischer Oberfläche: 700 MB Hier kann zumindest X11 mit einigen Anwendungen installiert werden.

Standard-System: 1.5 GB Hier können die modernen Desktop-Oberflächen wie KDE oder GNOME installiert werden. Auch „große" Anwendungen wie Netscape oder Mozilla sind kein Problem.

Vollinstallation 2.5 GB Hier können alle Software-Pakete installiert werden.

Die Aufteilung des Speicherplatzes hängt stark ab vom Verwendungszweck des installierten Computers, aber es gibt Anhaltspunkte:

Bis ca. 4 GB: Eine Swap-Partition und eine Root-Partition (`/`). Die Root-Partition nimmt dann auch jene Verzeichnisse auf, für die bei größeren Festplatten oft eigene Partitionen verwendet werden.

Vorschlag ab 4 GB: Swap, Root (1 GB) und ggf. je eine Partition für `/usr` (4 GB oder größer), `/opt` (4 GB oder größer) und `/var` (1 GB). Der Rest des freien Platzes kann dann für `/home` vorgesehen werden.

Abhängig von der Hardware des Computers kann es notwendig sein, eine Boot-Partition für die Start-Dateien und den Linux-Kernel am Anfang der Festplatte einzurichten (`/boot`). Diese Partition sollte mindestens 8 MB groß sein bzw. einen (1) Zylinder umfassen. Als Faustregel gilt: Wenn YaST eine Boot-Partiton vorschlägt, sollten Sie auch bei manueller Partitionierung eine solche vorsehen. In Zweifelsfällen ist es am sichersten, eine Boot-Partition anzulegen.

Weiterhin ist zu bedenken, dass einige — zumeist kommerzielle — Programme ihre Daten unter `/opt` installieren; sehen Sie ggf. entweder für `/opt` eine eigene Partition vor oder dimensionieren Sie die Root-Partition entsprechend größer.

Partitionierung mit YaST

Wenn Sie im Vorschlags-Dialog erstmalig die Partitionierung anwählen, erscheint der YaST-Partitionierungs-Dialog mit den aktuellen Einstellungen. Sie können diese Einstellungen hier übernehmen, abändern oder komplett verwerfen und eine ganz neue Aufteilung vornehmen.

Abbildung 1.10: *Partitionierungsvorschlag bearbeiten*

Wenn Sie 'Den Vorschlag für die Partitionierung übernehmen' anwählen, werden keine Änderungen vorgenommen, der Vorschlags-Dialog bleibt unverändert. Wenn Sie 'Den Vorschlag für die Partitionierung abändern' anwählen, erscheint direkt der Experten-Dialog, der es erlaubt, sehr detaillierte Einstellungen vorzunehmen (siehe Abschnitt 1.7.5 auf Seite 24). Der von YaST ermittelte Partitionierungs-Vorschlag ist dann bereits dort eingetragen und kann bearbeitet werden.

Wenn Sie 'Partitionen nach eigenen Vorstellungen anlegen' anwählen, erscheint zunächst ein Dialog für die Auswahl der Festplatte (Abb. 1.11 auf der nächsten Seite). Alle in Ihrem System vorhandenen Festplatten sind hier aufgelistet. Wählen Sie jene aus, auf der Sie SUSE LINUX installieren möchten.

Nach der Auswahl einer Festplatte können Sie zunächst bestimmen, ob die 'Gesamte Festplatte', verwendet werden soll oder ob nur einzelne Par-

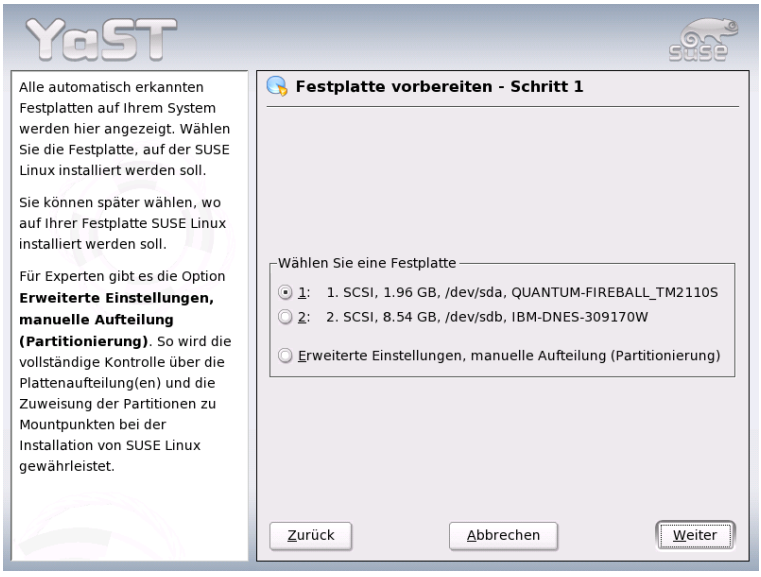

Abbildung 1.11: *Auswählen der Festplatte*

titionen (falls schon vorhanden) dafür freigegeben werden sollen. Wenn die gewählte Festplatte ein Windows-Betriebssystem enthält, werden Sie hier ggf. gefragt, ob Sie Windows löschen oder verkleinern wollen. Lesen Sie in diesem Fall bitte den Abschnitt 1.7.5 auf Seite 27. Andernfalls kommen Sie von hier aus ebenfalls zum Experten-Dialog, wo Sie Ihre Wunsch-Partitionierung einstellen können (siehe Abschnitt 1.7.5 auf der nächsten Seite).

Achtung

Gesamte Festplatte zur Installation freigeben

Bei der Auswahl ‘Gesamte Festplatte’ gehen später sämtliche vor der Installation auf dieser Festplatte vorhandenen Daten verloren.

Achtung

Im weiteren Verlauf der Installation überprüft YaST, ob der Festplattenplatz für die aktuelle Software-Auswahl ausreicht. Falls dies nicht der Fall ist, wird u. U. die aktuelle Software-Auswahl automatisch geändert. Der

Vorschlags-Dialog enthält dann einen entsprechenden Hinweis. Steht genügend Speicherplatz zur Verfügung, wird YaST Ihre Einstellungen übernehmen und den zugewiesenen Platz auf der Festplatte aufteilen.

1.7.5 Experten-Partitionierung mit YaST

Im Experten-Dialog (Abbildung 1.12) können Sie manuell die Partitionierung Ihrer Festplatte(n) ändern. Sie können Partitionen hinzufügen, löschen oder bearbeiten.

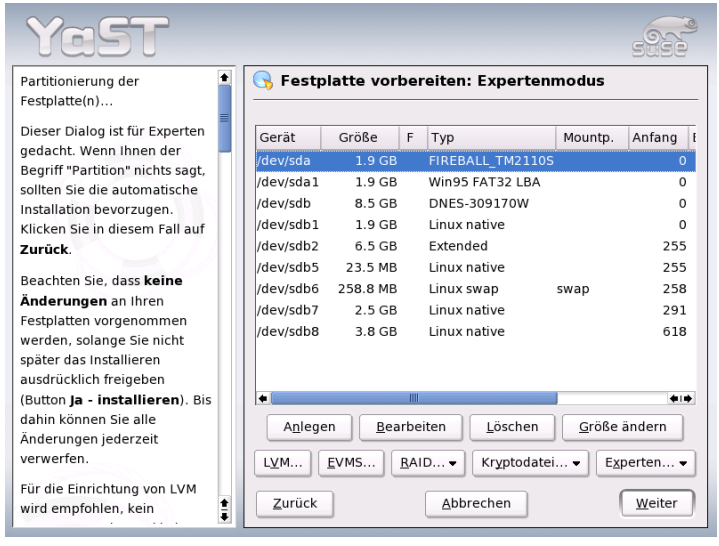

Abbildung 1.12: *Der YaST-Partitionierer im Experten-Modus*

Hinweis

S/390, zSeries: Gerätenamen auf IBM S/390 und zSeries

IBM S/390 und zSeries kennen nur DASDs und SCSI-Festplatten. IDE-Festplatten sind nicht unterstützt. Dementsprechend erscheinen diese Geräte mit den Einträgen `dasda` bzw. `sda` für das jeweils erste erkannte Gerät in der Partitionstabelle.

Hinweis

In der Liste des Experten-Dialogs werden alle schon vorhandenen bzw. vorgeschlagenen Partitionen auf allen angeschlossenen Festplatten angezeigt. Ganze Platten sind als Geräte ohne Nummern dargestellt (zum Beispiel `/dev/hda` oder `/dev/sda` bzw. `/dev/dasda`), während einzelne Partitionen als Teile dieser Geräte numeriert dargestellt sind (zum Beispiel `/dev/hda1` oder `/dev/sda1` bzw. `/dev/dasda1`). Von den Platten und den Partitionen werden Größe, Typ, Dateisystem und Mountpunkt als wichtige Parameter angezeigt. Der Mountpunkt beschreibt, wo die Partition im Dateibaum von Linux eingehängt ist.

Der freie Festplattenplatz wird (falls vorhanden) ebenfalls angezeigt und automatisch als gewählt gekennzeichnet. Wenn Sie Linux weiteren Speicherplatz zur Verfügung stellen wollen, können Sie ihn in der Liste von unten nach oben, das heisst, in der Reihenfolge von der letzten bis hin zur ersten Partition einer Festplatte freigeben. Es ist jedoch nicht möglich, zum Beispiel bei drei Partitionen ausschließlich die zweite für Linux zu wählen und die dritte und die erste Partition daneben für andere Betriebssysteme zu erhalten.

Partition erstellen

Wählen Sie ‘Neu’. Wenn mehrere Festplatten angeschlossen sind, erscheint zunächst ein Auswahl-Dialog, in dem Sie eine Platte für die neue Partition auswählen können. Danach legen Sie den Typ der Partition (primär oder erweitert) fest. Sie können bis zu vier primäre oder drei primäre und eine erweiterte Partition erstellen. In der erweiterten Partition können Sie wiederum mehrere logische Partitionen erstellen (siehe Kap. 1.7.4 auf Seite 20).

Wählen Sie dann das Dateisystem, mit dem die Partition formatiert werden soll und, wenn nötig, einen Mountpunkt. YaST schlägt Ihnen zu jeder Partition, die Sie anlegen, einen Mountpunkt vor. Details zu den Parametern finden Sie im nächsten Absatz.

Wählen Sie ‘OK’, damit die Änderungen wirksam werden. Die neue Partition wird nun in der Partitionstabelle aufgelistet. Wenn Sie auf ‘Weiter’ klicken, werden die aktuellen Werte übernommen und der Vorschlags-Dialog erscheint wieder.

Parameter beim Partitionieren

Wenn Sie eine neue Partition erstellen oder eine bestehende Partition ändern, können Sie verschiedene Parameter im Partitionierer setzen. Bei neu angelegten Partitionen werden diese Parameter von YaST sinnvoll gesetzt und müssen normalerweise nicht geändert werden. Falls Sie dennoch manuell eingreifen wollen, gehen Sie folgendermaßen vor:

1. Auswählen der Partition
2. 'Bearbeiten' der Partition und Setzen der Parameter:
   - Dateisystem-Kennung
     Wenn Sie die Partition vorerst nicht formatieren wollen, müssen Sie hier zumindest die Dateisystem-ID angeben, damit die Partition korrekt eingetragen werden kann. Mögliche Werte sind hier zum Beispiel 'Linux', 'Linux swap', 'Linux LVM' und 'Linux RAID'. Details zu LVM und RAID finden Sie in den Abschnitten 3.10 auf Seite 152 und 3.11 auf Seite 160.
   - Dateisystem
     Wenn Sie die Partition gleich im Rahmen der Installation formatieren wollen, können Sie hier angeben, welches Dateisystem die Partition erhalten soll. Mögliche Werte sind hier zum Beispiel 'Swap', 'Ext2', 'Ext3', 'ReiserFS' und 'JFS'.
   - Dateisystem-Optionen
     Hier können Sie verschiedene Arbeitsparameter des gewählten Dateisystems einstellen.
   - Dateisystem verschlüsseln
     Wenn Sie die Verschlüsselung aktivieren, werden alle Daten verschlüsselt auf die Festplatte geschrieben.
   - Fstab-Optionen
     Hier können Sie verschiedene Parameter für die Verwaltungsdatei der Dateisysteme (`/etc/fstab`) angeben.
   - Mountpunkt
     Gibt jenes Verzeichnis an, in dem die Partition in den Dateisystembaum eingehängt werden soll. Am entsprechenden Eingabefeld können verschiedene YaST-Vorschläge ausgeklappt werden, die bei Verwendung Ihr Dateisystem dem Standard entsprechend strukturieren; Sie können aber auch beliebige eigene Namen vergeben.
3. Wählen Sie 'Weiter', um die Partition aktivieren.

Wenn Sie manuell partitionieren, müssen Sie eine Swap-Partition anlegen. Der Swap-Bereich dient dazu, momentan nicht benötigte Daten aus dem Hauptspeicher auszulagern, um den Arbeitsspeicher immer für die wichtigsten, gegenwärtig am häufigsten gebrauchten Daten frei zu halten.

Hinweis

S/390, zSeries: Weitere Schritte

Weitere, für IBM S/390 und zSeries relevante Informationen lesen Sie im Abschnitt 1.7.5 auf Seite 31 nach.

Hinweis

Anpassen einer Windows-Partition

Wenn im Rahmen der Partitionierung eine Festplatte mit Windows-FAT-Partition oder Windows-NTFS-Partition als Installationsziel ausgewählt wurde, bietet YaST Ihnen ggf. an, diese Partition zu löschen oder zu verkleinern. Auf diese Weise können Sie SUSE LINUX auch dann installieren, wenn auf der Festplatte nicht genügend Platz frei ist. Dies ist besonders dann sinnvoll, wenn auf der ausgewählten Festplatte nur eine einzige Partition mit Windows existiert, was bei manchen vorinstallierten Rechnern der Fall ist.

Wenn YaST erkennt, dass auf der gewählten Festplatte zuwenig Patz für die Installation vorhanden ist, und dieses Problem durch Löschen oder Verkleinern einer Windows-Partition behoben werden könnte, erscheint ein entsprechender Dialog zur Auswahl der gewüschten Option.

Wenn Sie 'Windows komplett löschen' anwählen, wird die Windows-Partition zum Löschen markiert, und der dadurch frei gewordene Platz für die Installation von SUSE LINUX verwendet.

Achtung

Windows löschen

Beim Löschen von Windows sollten Sie beachten, dass alle Windows-Daten später bei der Formatierung unwiederbringlich verloren gehen.

Achtung

Wenn Sie sich entscheiden, Ihre Windows-Partition zu verkleinern, sollten Sie zunächst die Installation abbrechen und Windows booten, um dort einige vorbereitende Schritte auszuführen. Dies ist bei FAT-Partitionen zwar nicht unbedingt notwendig, aber es beschleunigt in diesem Fall den Verkleinerungsprozess und macht ihn sicherer. Für NTFS-Partitionen sind diese Schritte zwingend notwendig.

Abbildung 1.13: *Mögliche Optionen bei Windows-Partitionen.*

FAT-Dateisystem Führen Sie zunächst in Windows das Programm scandisk aus, um sicherzustellen, dass das FAT-Dateisystem frei von Verkettungsfehlern ist. Anschließend schieben Sie mit defrag die Dateien an den Anfang der Partition, wodurch der spätere Verkleinerungsprozess unter Linux beschleunigt wird.

Falls Sie eine Windows-Swap-Optimierung mit zusammenhängender Swap-Datei bei gleicher Ober- und Untergrenze für die Größe eingerichtet haben, ist ein weiterer Vorbereitungsschritt sinnvoll. In diesem Fall kann es nämlich sein, dass die Swap-Datei beim Verkleinern zerstückelt und über die gesamte Windows-Partition verstreut wird. Weiterhin muss in diesem Fall die Swap-Datei beim Verkleinern mitverschoben werden, was den Verkleinerungsprozess verlangsamt. Sie sollten eine solche Optimierung daher vor der Verkleinerung aufheben und danach erneut durchführen.

NTFS-Dateisystem Auch hier führen Sie zunächst in Windows die Programme scandisk und defrag aus, um die Dateien an den Anfang der Festplatte zu verschieben. Im Gegensatz zum FAT-Dateisystem

muss dies bei NTFS unbedingt erfolgen, damit die Verkleinerung durchgeführt werden kann.

Hinweis

Windows-Swap verkleinern

Wenn Sie Ihr System mit einer permanenten Swap-Datei auf einem NTFS-Dateisystem betreiben, kann es sein, dass diese Datei am Ende der Festplatte liegt und dort trotz defrag auch verbleibt. Dies kann dazu führen, dass die Partition nicht ausreichend verkleinert werden kann. Schalten Sie bitte in diesem Fall in Windows die Swap-Datei (den virtuellen Speicher) vorübergehend ab. Nach der Verkleinerung der Partition können Sie dann wieder beliebig viel virtuellen Speicher einrichten.

Hinweis

Wenn Sie nach dieser Vorbereitung wieder bei der Partitionierung angelangt sind, wählen Sie im oben genannten Dialog 'Windows-Partition verkleinern'. Nach einer kurzen Prüfung der Partition öffnet YaST einen neuen Dialog mit einem Vorschlag zur sinnvollen Verkleinerung der Windows-Partition.

Im ersten Balkendiagramm sehen Sie, wieviel Speicherplatz Windows aktuell belegt und wieviel Festplattenspeicher noch frei ist. Das zweite Diagramm stellt den YaST-Vorschlag für die neue Aufteilung der Festplatte dar. (Abbildung 1.14 auf der nächsten Seite). Sie können diesen Vorschlag übernehmen oder die Grenzen mit dem Schieber darunter weitgehend frei verändern.

Wenn Sie diesen Dialog mit 'Weiter' verlassen, werden die aktuellen Einstellungen gespeichert und Sie kehren zum vorherigen Dialog zurück. Die Verkleinerung findet nicht sofort statt, sondern erst später, bevor die Festplatte formatiert wird.

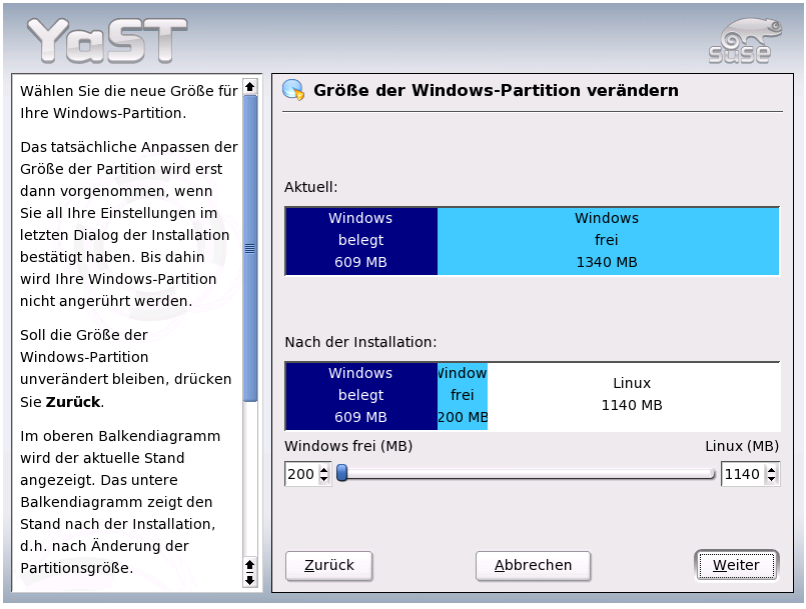

Abbildung 1.14: *Anpassen der Windows-Partition.*

Hinweis

Windows mit NTFS-Dateisystem

Die Windows-Versionen NT, 2000 und XP verwenden als Standard das NTFS-Dateisystem. Im Gegensatz zu FAT-Dateisystemen können auf NTFS-Dateisysteme (aktuell) von Linux aus nur lesend zugegriffen werden. Sie können daher mit NTFS unter Linux Ihre Windows-Dateien zwar lesen, nicht aber verändern. Wenn Sie auf Ihre Windows-Daten auch schreibend zugreifen möchten und das NTFS-Dateisystem nicht unbedingt verwenden wollen, können Sie Windows auf einem FAT-32-Dateisystem neu installieren. Sie haben dann von SUSE LINUX aus vollen Zugriff auf Ihre Windows-Daten.

Hinweis

Weitere Hinweise zum Partitionieren

Wenn YaST automatisch die Partitionierung vornimmt und dabei erkennt, dass sich andere Partitionen im System befinden, werden diese auch in der Datei `/etc/fstab` eingetragen, um später im installierten System einen einfachen Zugriff auf diese Daten zu ermöglichen. In dieser Datei stehen alle im System befindlichen Partitionen mit ihren zugehörigen Eigenschaften (Parametern) wie Dateisystem, Mountpunkt und Nutzerrechte.

Beispiel 1.1: */etc/fstab: data-Partitionen*

```
/dev/sda1       /data1  auto    noauto,user 0 0
/dev/sda8       /data2  auto    noauto,user 0 0
/dev/dasda1     /data3  auto    noauto,user 0 0
```

Die Partitionen, egal ob Linux- oder FAT-Partitionen, werden mit den Optionen `noauto` und `user` eingetragen. So kann jeder Benutzer diese Partitionen bei Bedarf ein- oder aushängen. Aus Gründen der Sicherheit wird von YaST hier nicht die Option `exec` eingetragen, die notwendig ist, damit Programme von dort ausgeführt werden können. Falls Sie hier dennoch Programme oder Skripten ausführen wollen, tragen Sie diese Option bitte manuell nach. Diese Maßnahme ist spätestens dann notwendig, wenn Sie Meldungen wie "bad interpreter" oder "Permission denied" zu sehen bekommen.

Viele weitere ausführliche Hintergrundinformationen und Tipps zum Partitionieren finden Sie im Abschnitt 3.9 auf Seite 148.

1.7.6 Software

SUSE LINUX enthält sehr viele Software-Pakete für die verschiedensten Anwendungsbereiche, die je nach Verwendungszweck installiert werden können. Da es sehr mühsam wäre, aus der Unmenge von Paketen die gewünschten einzeln auszuwählen, bietet SUSE LINUX bei der Installation verschiedene System-Typen mit unterschiedlichem Installationsumfang an. Entsprechend dem verfügbaren Speicherplatz hat YaST bereits eines dieser Grundsysteme ausgewählt und im Vorschlagsdialog angezeigt.

Minimales System (Nur für Spezialanwendungen empfehlenswert)
: Hier wird im Wesentlichen nur das Betriebssystem mit verschiedenen Diensten installiert. Es gibt keine grafische Oberfläche; der Rechner ist nur über die ASCII-Konsolen bedienbar. Dieser System-Typ eignet sich v.a. für Server-Anwendungen, die kaum direkte Benutzer-Interaktion erfordern.

Minimales graphisches System (ohne KDE)
Wenn der komfortable KDE-Desktop nicht gewünscht wird oder dafür zu wenig Speicherplatz vorhanden ist, kann dieser System-Typ installiert werden. Das installierte System enthält eine elementare graphische Oberfläche mit einem Window-Manager. Es können alle Programme mit eigenen grafischen Oberflächen genutzt werden.

Standardsystem (mit KDE) Dieses System enthält den KDE-Desktop mit den meisten KDE-Programmen und den `CUPS` Print Server. Dieser System-Typ ist für Einzelplatzrechner mit üblicher Nutzung am besten geeignet. Er wird von YaST ausgewählt, wenn die Rahmenbedingungen es erlauben.

Vollinstallation Dieses System enthält eine möglichst umfangreiche konfliktfreie Selektion von Paketen in der gewählten Sprache. Es ist das größte der angebotenen Grundsysteme.

Wenn Sie im Vorschlagsdialog auf 'Software' klicken, erscheint ein Dialog, in dem Sie aus den o.g. Grundsystemen eines auswählen können. Zusätzlich können Sie durch einen Klick auf 'Detaillierte Auswahl' das Softwareinstallationsmodul (kurz: Paket-Manager) starten und dort den Installationsumfang detailliert ändern (s. Abb. 1.15 auf der nächsten Seite).

Vorgewählten Installationsumfang ändern

Bei der Installation des „Standard-Systems“ ist es meist nicht nötig, den Installationsumfang auf der Ebene einzelner Pakete zu verändern. Dieses Grundsystem bestimmt bereits eine in sich schlüssige Software-Zusammenstellung, die ohne weitere Änderungen die meisten Anforderungen erfüllt. Falls Sie dennoch manuell eingreifen möchten, erleichtert Ihnen der Paket-Manager diese Aufgabe erheblich. Er bietet sog. Filter an, die aus den vielen Paketen in SUSE LINUX eine Auswahl nach wählbaren Kriterien treffen.

Links oben, unter der Menüzeile, sehen Sie die Filter-Auswahlbox. Beim Start ist der Selektionen-Filter aktiviert. Selektionen gruppieren die Programmpakete nach Anwendungszweck, zum Beispiel Multimedia oder Büroanwendungen. Unter der Filter-Auswahlbox sehen Sie die verschiedenen Gruppen des Selektionen-Filters, von denen jene schon ausgewählt sind, die zum aktuell gewählten System-Typ gehören (Vorauswahl). Mit einem Klick auf die jeweilige Checkbox können ganze Selektionen zum Installieren komplett an- und abgewählt werden.

Im rechten Fenster sehen Sie jene Pakete einzeln aufgelistet, die zur aktuellen Selektion gehören. Alle Pakete haben einen aktuellen Status, der am

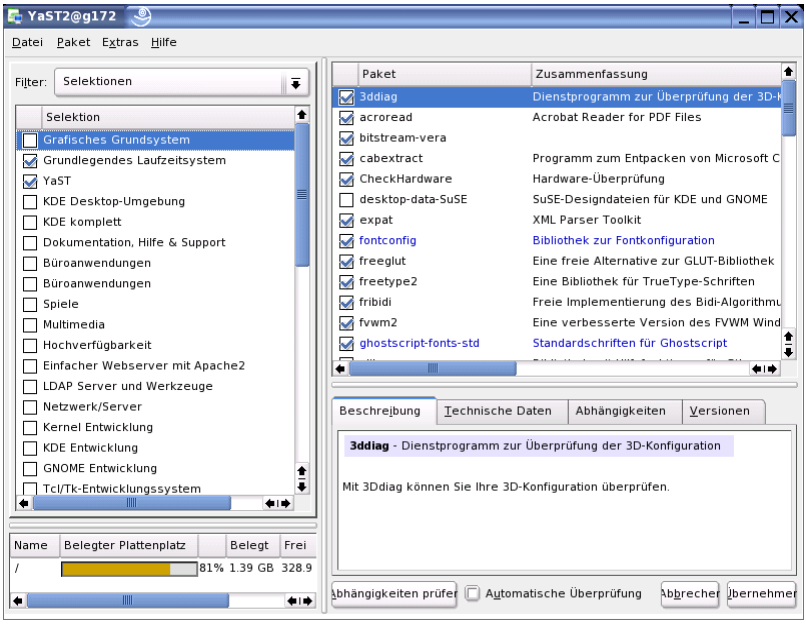

Abbildung 1.15: *YaST: Software installieren oder löschen (Paket-Manager)*

Anfang der Zeile in einer kleinen Status-Box symbolisch dargestellt wird. Bei der Installation sind vor allem die Zustände ‘Installieren’ und ‘Nicht installieren’ interessant, also mit Häkchen links vom Paketnamen oder mit Leerfeld. Hier können Sie jedes einzelne Paket nach Ihren Bedürfnissen an- oder abwählen. Klicken Sie dazu so oft auf die Status-Box, bis der jeweilige Zustand erreicht ist (Installieren oder Nicht installieren).

Alternativ können Sie mit einem Klick der rechten Maustaste auf die Paketzeile ein Popup-Menü aufrufen, das alle möglichen Zustände auflistet. Die übrigen Zustände sind zum Installieren aber weniger von Belang. Sie werden in der detaillierten Anleitung zu diesem Modul im Abschnitt 2.3.4 auf Seite 59 genauer erklärt.

Andere Filter

Wenn Sie die Filter-Auswahlbox aufklappen, sehen Sie eine Auswahl der möglichen Filter. Für die Installation ist auch die Auswahl nach ‘Paketgruppen’ interessant. Mit diesem Filter werden die Programmpakete auf

der linken Seite in einer Baumstruktur nach Themen geordnet. Je weiter Sie diesen Baum in die Tiefe hinein aufklappen, desto schärfer ist die Eingrenzung der Auswahl auf ein bestimmtes Thema. Die Liste der zugehörigen Pakete rechts in der Paketliste wird dadurch immer kürzer und überschaubarer.

Mit 'Suche' können Sie nach einem speziellen Paket suchen. Wie dies genau funktioniert, wird ebenfalls im Abschnitt 2.3.4 auf Seite 59 genauer erklärt.

Paketabhängigkeiten und -Konflikte

Wie in allen Betriebssystemen gilt auch bei SUSE LINUX, dass nicht beliebige Kombinationen von Software-Paketen installiert werden können. Die installierten Pakete müssen zueinander passen. Wird dies nicht beachtet, können sich Inkonsistenzen ergeben, die eine reibungslose Funktion des installierten Systems gefährden. Wenn Sie in diesem Dialog Software-Pakete an- und abwählen, können u.U. Warnungen über unaufgelöste Paket-Abhängigkeiten oder -Konflikte angezeigt werden. Falls Sie SUSE LINUX zum ersten Mal installieren oder diese Warnungen unverständlich für Sie sind, lesen Sie bitte den Abschnitt 2.3.4 auf Seite 59. Dort finden Sie detaillierte Informationen zur Bedienung des Paket-Managers.

Software-Auswahl beenden

Wenn Sie mit Ihrer Software-Auswahl zufrieden sind und keine unaufgelösten Paket-Abhängigkeiten oder -Konflikte mehr vorliegen, können Sie mit einem Klick auf 'Akzeptieren' Ihre Änderungen übernehmen und das Programm verlassen. Anders als beim Aufruf dieses Moduls im installierten System werden Ihre Änderungen während der Installation nicht sofort realisiert. Der aktuelle Installationsumfang wird nur intern vermerkt und wirkt sich erst später aus, wenn die Installation tatsächlich startet.

1.7.7 System-Start (Bootloader-Installation)

Hinweis

S/390, zSeries: Bootloader-Konfiguration

Das im Folgenden beschriebene Modul kann auf IBM S/390 und zSeries nicht zur Konfiguration des Bootloaders (zipl) eingesetzt werden.

Hinweis

Der Boot-Modus wird von YaST bei der Installation auf eine sinnvolle Weise festgelegt und Sie können diese Einstellungen normalerweise unverändert übernehmen. Sollten spezielle Anforderungen Ihrer Systemumgebung dafür sprechen, die vorgeschlagene Konfiguration zu ändern, ist dies aber auch möglich.

Sie können die Konfiguration zum Beispiel so ändern, dass zum Booten von SUSE LINUX eine spezielle Start-Diskette eingelegt werden muss. Das kann in Ausnahmefällen sinnvoll sein, wenn hauptsächlich ein anderes Betriebssystem gestartet wird, dessen aktueller Boot-Mechanismus unverändert bleiben soll. Normalerweise ist dies aber nicht notwendig, weil YaST den Bootloader so einrichtet, dass ein evtl. koexistierendes Betriebssystem wahlweise gebootet werden kann. Weiterhin können Sie den Speicherort des SUSE LINUX-Bootloaders auf der Festplatte ändern.

Wenn Sie den YaST-Vorschlag ändern möchten, wählen Sie bitte 'Systemstart'. Es erscheint dann ein Dialog, der weitreichende Eingriffe in den Boot-Mechanismus erlaubt. Lesen Sie hierzu bitte das Kapitel 8.6 auf Seite 244.

1.7.8 Zeitzone

In diesem Dialog (Abb. 1.16 auf der nächsten Seite) können Sie im Feld 'Rechneruhr einstellen auf' zwischen `Lokalzeit` und `UTC` (*Universal Time Coordinated*) wählen. Ihre Auswahl hängt von der Einstellung der Uhr im BIOS Ihres Rechners ab. Sollte diese auf `UTC` stehen, übernimmt SUSE LINUX automatisch die Umstellung von Sommer- auf Winterzeit und umgekehrt.

1.7.9 Sprache

Die Sprache wurde bereits am Beginn der Installation ausgewählt (siehe Abschnitt 1.4 auf Seite 13). Wenn Sie aber nachträglich noch Änderungen vornehmen wollen, können Sie dies hier tun. Zusätzlich haben Sie die Möglichkeit, über den Button 'Details' die Sprache für den Benutzer `root` einzustellen. Das Drop-down-Menü bietet drei Optionen:

ctype Für den Benutzer `root` wird der Wert der Variable `LC_CTYPE` in der Datei `/etc/sysconfig/language` übernommen. Damit wird die Lokalisierung für sprachabhängige Funktionsaufrufe gesetzt.

yes Benutzer `root` hat exakt dieselben Spracheinstellungen wie der lokale Benutzer.

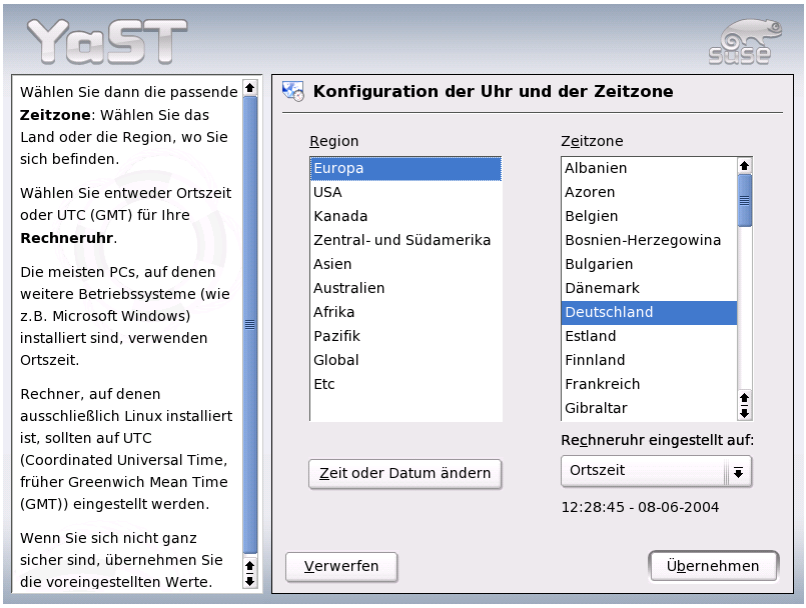

Abbildung 1.16: *Auswählen der Zeitzone*

no Die Spracheinstellungen für den Benutzer `root` bleiben von der Sprachauswahl unberührt.

Klicken Sie auf ‘OK’, um die Konfiguration abzuschließen. Über den Button ‘Verwerfen’ können Sie Ihre Änderungen ggf. wieder rückgängig machen.

1.7.10 Installation durchführen

Im Vorschlags-Dialog nehmen Sie mit einem Klick auf ‘Weiter’ den Vorschlag mit all Ihren Änderungen an und gelangen in den grünen Bestätigungsdialog. Wenn Sie hier nun ‘Ja’ wählen, beginnt die Installation unter Berücksichtigung aller aktuellen Einstellungen. Je nach Rechnerleistung und Software-Auswahl dauert das Kopieren der Pakete meist zwischen 15 und 30 Minuten. Nach Installation der Pakete bootet YaST das installierte System, bevor Sie mit der Hardware- und Dienstekonfiguration fortfahren können.

1.7.11 S/390, zSeries: IPL des installierten Systems

Nach Installation der ausgewählten Softwarepakete muss erneut ein IPL des IBM S/390 oder zSeries Systems durchgeführt werden. Je nach gewähltem Installationstyp unterscheidet sich das Vorgehen:

ESA Native und LPAR Installation
Wählen Sie an der HMC der IBM S/390 oder zSeries 'LOAD' und 'Clear' und geben Sie anschließend die Ladeadresse (die Device-Adresse Ihres Root-Devices) ein. Verwenden Sie eine ZFCP-Platte als Boot-Device, wählen Sie 'LOAD from SCSI' und geben zusätzlich ZFCP-WWPN und LUN des Boot-Devices an. und Starten Sie nun den Ladeprozess.

z/VM Installation Fahren Sie das Installationssystem mit `halt` herunter. Melden Sie sich am VM-Gast als Benutzer `LINUX1` an und nehmen Sie den IPL des installierten Systems vor. Verwenden Sie eine ZFCP-Platte als Boot-Device, müssen Sie die ZFCP-WWPN und LUN spezifizieren, bevor Sie den IPL vornehmen können. Beachten Sie hierbei, dass die Parameter maximal acht Stellen lang sein können; längere Zahlen müssen durch Leerzeichen voneinander getrennt werden:

```
SET LOADDEV PORT 50050763 00C590A9 LUN 50010000 00000000
```

Anschließend führen Sie den IPL durch:

```
IPL 151 CLEAR
```

1.7.12 S/390, zSeries: Verbindungsaufbau zum installierten System

Nachdem der IPL des installierten Systems erfolgt ist, bauen Sie eine Verbindung zum installierten System auf, um die Installation abzuschließen. Das konkrete Vorgehen hängt von der ursprünglich gewählten Verbindungsmethode ab.

Verbindungsaufbau mit VNC

Eine Meldung im 3270-Terminal bittet Sie, sich mittels eines VNC-Clients mit dem Linux-System verbinden. Diese Meldung kann leicht übersehen werden, da sie zwischen Kernelmeldungen eingeschoben wird oder sich

das Terminal beendet, ehe Sie diese Meldung wahrnehmen konnten. In diesem Fall verbinden Sie sich per VNC-Viewer mit dem Linux-System, falls für mehr als fünf Minuten nichts passieren sollte.

Wenn Sie die Verbindung mittels eines Java-fähigen Browsers aufbauen, geben Sie eine URL, die die IP-Adresse des Installationssystems und die passende Portnummer enthält ein:

```
http://<IP Adresse  des Installationssystems>:5801/
```

Verbindungsaufbau mit X

Stellen Sie sicher, dass der X Server auf demselben System läuft, das auch zur Installation verwendet wurde, wenn Sie den IPL des installierten Systems ausführen. Ein YaST Fenster erscheint und die Installation wird beendet.

Verbindungsaufbau mit SSH

Hinweis

S/390, zSeries: Verbindungsaufbau von einem Linux- oder Unix-System

Starten Sie ssh aus einem xterm. Anderen Terminalemulationen mangelt es an vollständiger Unterstützung der textbasierten YaST Oberfläche.

Hinweis

Eine Meldung im 3270-Terminal bittet Sie, sich mittels eines SSH-Clients mit dem Linux-System verbinden. Diese Meldung kann leicht übersehen werden, da sie zwischen Kernelmeldungen eingeschoben wird oder sich das Terminal beendet, ehe Sie diese Meldung wahrnehmen konnten.

Führen Sie nun die folgenden Schritte aus, um die Installation abzuschließen:

- Verwenden Sie ssh, um sich am Linux-System als `root` anzumelden. Sollte die Verbindung einen Timeout bekommen oder der Verbindungsaufbau abgelehnt werden, versuchen Sie wenige Minuten später erneut.
- Führen Sie das folgende Kommando aus:

  ```
  /usr/lib/YaST2/bin/YaST2.sshinstall
  ```

  (ein bloßes `yast` reicht hier nicht aus)

YaST wird nun gestartet und mit der Installation der verbliebenen Pakete fortfahren und die initiale Systemkonfiguration vornehmen.

1.8 Installation abschließen

Nachdem das System und Ihre ausgewählte Software fertig installiert sind, müssen Sie noch ein Passwort für den Systemadministrator (Benutzer `root`) festlegen. Anschließend bekommen Sie Gelegenheit, gleich im Rahmen der Installation einen Internet-Zugang und eine Netzwerkverbindung zu konfigurieren. Auf diese Weise ist es möglich, schon während der Installation Software-Updates für SUSE LINUX anzuwenden und ggf. Namensdienste für die zentrale Verwaltung der Benutzer in einem Netzwerk einzurichten. Zum Abschluss können Sie im neu installierten System Ihre angeschlossene Hardware konfigurieren.

1.8.1 Root-Passwort

Abbildung 1.17: *Passwort für den Benutzer root angeben*

Root ist der Name für den Superuser oder Administrator des Systems; `root` darf all das, was der normale Nutzer nicht darf. Er kann das System verändern, neue Programme installieren oder neue Hardware ein-

richten. Wenn ein Benutzer sein Passwort vergessen hat oder Programme nicht mehr laufen, hat `root` die Möglichkeit, zu helfen. Im Allgemeinen sollte man nur für administrative Aufgaben, Wartungs- und Reparaturarbeiten als `root` angemeldet sein. Für den Alltagsbetrieb ist dies riskant, da `root` zum Beispiel versehentlich System-Dateien unwiederbringlich löschen kann.

Bei der Passwortvergabe für `root` muss das Passwort zur Überprüfung zweimal eingegeben werden (Abb. 1.17 auf der vorherigen Seite). Merken Sie sich das Passwort für den Benutzer `root` besonders gut. Es kann zu einem späteren Zeitpunkt nicht mehr eingesehen werden.

1.8.2 Netzwerkkonfiguration

Hinweis

S/390, zSeries: Netzwerkkonfiguration

IBM S/390 und zSeries benötigen bereits zur Installation eine korrekt konfigurierte Netzwerkverbindung, um den Kontakt zwischen Installationssystem, Installationsquelle und dem YaST Terminal zur Steuerung des Prozesses aufzubauen. Das Vorgehen hierzu wird im Kapitel *Netzwerkkonfiguration* im *Architekturspezifika* Handbuch beschrieben. IBM S/390 und zSeries unterstützen ausschließlich die dort genannten Typen von Netzwerkschnittstellen (OSA Token Ring, OSA Ethernet, OSA Gigabit Ethernet, OSA Express Fast Ethernet, Escon, IUCV, OSA Express High-Speed Token Ring). Im YaST Dialog wird die bereits konfigurierte Schnittstelle angezeigt, deren Einstellungen übernommen werden können.

Hinweis

Im nächsten Schritt konfigurieren Sie die Netzwerkverbindung Ihres Systems. Wenn Ihr System über derartige Hardware verfügt, sollten Sie gleich hier von dieser Möglichkeit Gebrauch machen. Im weiteren Verlauf kann YaST dann ggf. Updates für SUSE LINUX aus dem Internet laden, die bei der Installation berücksichtigt werden.

Falls Sie Ihre Netzwerk-Hardware hier konfigurieren wollen, schlagen Sie bitte die entsprechenden Abschnitte im Kapitel 2.5 auf Seite 98 nach. Falls nicht, wählen Sie den Punkt 'Netzwerk-Einrichtung überspringen' und klicken auf 'Weiter'. Sie können die Netzwerk-Hardware dann später im installierten System konfigurieren.

Abbildung 1.18: *Konfiguration der Netzwerkgeräte*

1.8.3 Internet-Verbindung testen

Falls Sie eine Internet-Anbindung eingerichtet haben, können Sie diese hier gleich testen. Dazu stellt YaST eine Verbindung zum SUSE-Server her und prüft bei dieser Gelegenheit auch, ob Produkt-Updates für SUSE LINUX verfügbar sind. Sollte das der Fall sein, können Sie diese Updates im nächsten Schritt schon anwenden. Außerdem werden die neuesten Release-Notes vom SUSE-Server abgeholt. Am Ende der Installation werden diese Release-Notes dann am Bildschirm angezeigt.

Wenn Sie den Test der Internet-Verbindung hier nicht durchführen möchten, wählen Sie bitte ‘Test überspringen’ und klicken dann auf ‘Weiter’. Die Suche nach Produkt-Updates und das Laden der neuesten Release-Notes unterbleibt dann allerdings auch.

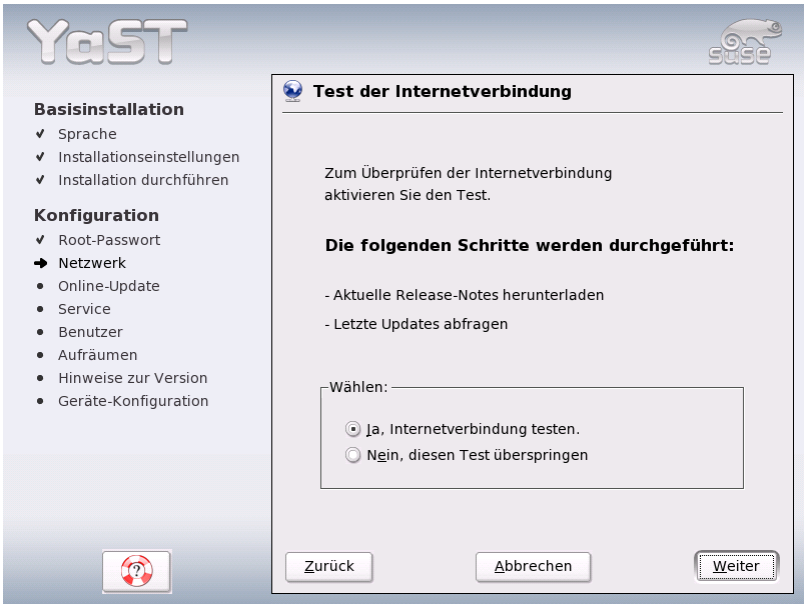

Abbildung 1.19: *Internet-Verbindung testen*

1.8.4 Software-Updates laden

Falls YaST im vorigen Schritt erfolgreich eine Internet-Verbindung herstellen konnte, wird Ihnen nun ggf. angeboten, ein YaST-Online-Update durchzuführen. Sollten auf dem SUSE-Server Patches vorliegen, die erkannte Fehler oder Sicherheitsprobleme beheben, können Sie diese hier anwenden.

Wenn Sie ein Software-Update sofort durchführen wollen, wählen Sie bitte ‘Update jetzt durchführen’ und klicken Sie auf ‘OK’. Sie gelangen dann in den Dialog des YaST-Online-Update und können dort die verfügbaren Patches sichten, auswählen und ggf. anwenden. Lesen Sie bitte in diesem Fall den Abschnitt 2.3.2 auf Seite 54. Sie können das Update aber natürlich auch jederzeit später im installierten System durchführen. Wählen Sie hierzu bitte ‘Update überspringen’ und klicken Sie auf ‘OK’.

1.8.5 Netzwerkdienste

Nach Test der Internet-Verbindung und dem Einspielen ersten Updates gelangen Sie in einen Dialog zur Aktivierung und Konfiguration zweier wichtiger Netzwerkdienste (siehe Abb. 1.20:

Abbildung 1.20: *Vorschlag: Netzwerkdienste*

CA-Management Eine CA (Certificate Authority) dient dazu, sicherzustellen, dass alle miteinander kommunizierenden Netzwerkdienste einander vertrauen können. Entscheiden Sie sich gegen die Einrichtung einer CA, muss die Absicherung der Serverkommunikation separat für jeden Dienst einzeln mit SSL/TLS erfolgen. Standardmäßig wird während der Installation eine CA eingerichtet und aktiviert. Details zur Einrichtung einer CA mit YaST und Hintergrundinformationen zu dieser Thematik finden Sie in 26.1 auf Seite 680.

LDAP-Server Der LDAP-Server kann auf Ihrem System zur zentralen Verwaltung verschiedener Konfiugarationsdateien eingesetzt werden. Typischerweise verwaltet ein LDAP-Server Benutzerinformationen, er kann unter SUSE LINUX Enterprise Server aber auch zur Verwaltung von Mail, DHCP und DNS-Informationen eingesetzt werden. Standardmäßig wird während der Installation ein LDAP-Server

eingerichtet. Entscheiden Sie sich gegen den Einsatz eines LDAP-Servers, wird das YaST Mailserver Modul nicht funktionieren, da es von LDAP-Funktionalitäten abhängig ist. In diesem Fall konfigurieren Sie den Mailverkehr auf Ihrem System über das Modul 'Mail Transfer Agent'. Mehr Details zu LDAP und zur Konfiguration mit YaST lesen Sie in Abschnitt 21.8 auf Seite 521 nach.

Wie auch die Konfiguration des Netzwerks kann auch dieser Konfigurationsvorschlag während des Installationsvorgans übersprungen werden und die betroffenen Dienste später im installierten System mit YaST konfiguriert und gestartet werden.

1.8.6 Benutzer-Authentifizierung

Wenn im Rahmen der Installation bereits ein funktionierender Netzwerkzugang konfiguriert wurde, haben Sie zwei Möglichkeiten, die Benutzer des neu installierten Systems zu verwalten.

NIS Die Benutzerdaten werden auf einem zentralen NIS-Server bereitgehalten.

Benutzerverwaltung LDAP Die Benutzerdaten werden auf einem zentralen LDAP-Server verwaltet.

Lokal (/etc/passwd) Diese Art der Konfiguration wird gewählt, wenn das System keinen Netzanschluss hat sich kein Benutzer von extern auf dem System einloggen soll. Die Benutzerverwaltung geschieht ausschließlich über die lokale Datei `/etc/passwd`.

Falls alle Voraussetzungen erfüllt sind, öffnet YaST einen Dialog zur Auswahl der geeigneten Methode (Abb. 1.21 auf der nächsten Seite). Wenn keine Netzwerkverbindung besteht, können Sie in jedem Fall lokale Benutzer anlegen.

1.8.7 Konfiguration als NIS-Client

Haben Sie sich entschieden, die Benutzerverwaltung über NIS abzuwickeln, müssen Sie im nächsten Schritt einen NIS-Client konfigurieren. An dieser Stelle wird lediglich die Konfiguration der Clientseite beschrieben, Informationen zur Konfiguration eines NIS-Servers mit YaST finden Sie in Abschnitt 21.9 auf Seite 553.

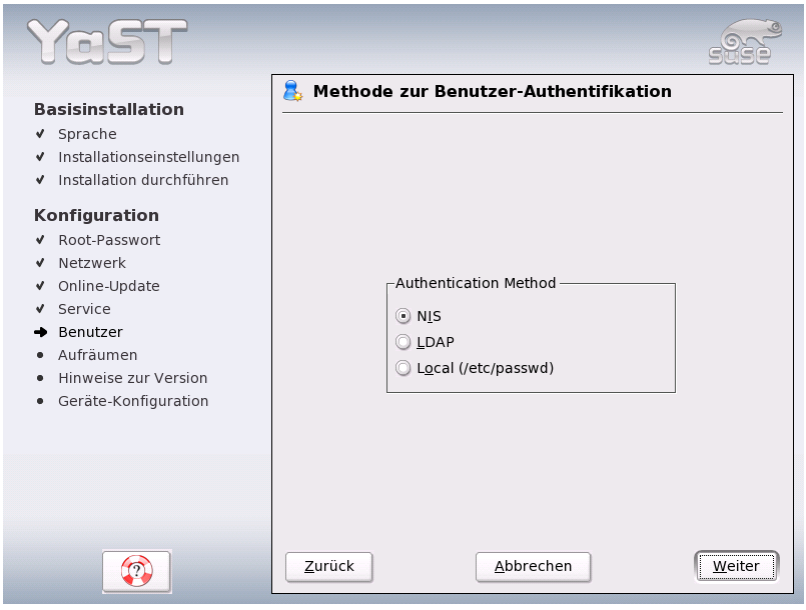

Abbildung 1.21: *Benutzer-Authentifizierung*

Im Dialog (Abb. 1.22 auf der nächsten Seite) geben Sie zunächst an, ob der NIS-Client eine statische IP-Adresse hat oder ob er diese über DHCP erhalten soll. In letzterem Fall können Sie keine NIS-Domain oder IP-Adresse des Servers angeben, da diese Daten ebenfalls über DHCP zugewiesen werden. Weitere Informationen zu DHCP finden Sie im Abschnitt 21.11 auf Seite 563. Falls der Client über eine statische IP-Adresse verfügt, müssen NIS-Domain und -Server manuell eingegeben werden.

Mit der Broadcast-Checkbox ermöglichen Sie die Suche nach einem NIS-Server im Netzwerk für den Fall, dass der angegebene Server nicht antwortet. Sie haben auch die Möglichkeit, mehrere Domains mit einer Default-Domain anzugeben. Für die einzelnen Domains wiederum können Sie mit ‘Hinzufügen’ mehrere Server einschließlich Broadcast-Funktion angeben.

In den Experten-Einstellungen können Sie mit der Option ‘Nur lokalem Host antworten’ verhindern, dass ein anderer Rechner im Netz abfragen kann, welchen Server Ihr Client benutzt. Wenn Sie ‘Fehlerhafter Server’ aktivieren, werden auch Antworten von einem Server auf einem unprivilegierten Port akzeptiert. Details dazu finden Sie in der Manual-Page von `ypbind`.

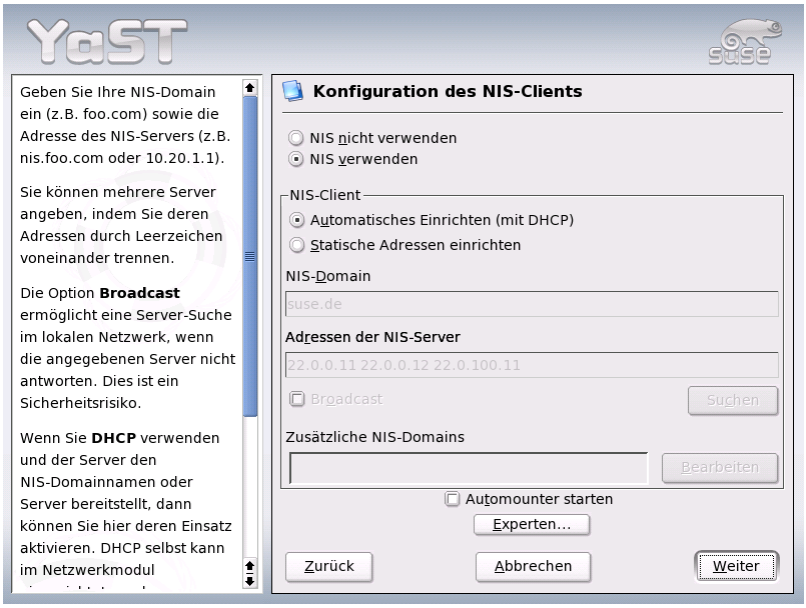

Abbildung 1.22: *NIS-Client-Konfiguration*

1.8.8 Lokale Benutzer anlegen

Falls Sie keine Namensdienst-basierte Benutzerauthentifizierung einrichten, bekommen Sie Gelegenheit, lokale Benutzer anzulegen. Die Daten dieser Benutzer (Name, Login, Passwort usw.) werden lokal auf dem installierten System abgelegt und verwaltet.

Linux ermöglicht mehreren Benutzern gleichzeitig das Arbeiten am System. Für jeden Benutzer muss ein Benutzerkonto angelegt werden, mit dem er sich am System anmeldet. Das Einrichten von Benutzerkonten bietet eine hervorragende Betriebssicherheit. So ist es zum Beispiel normalen Benutzern nicht möglich, wichtige Systemdateien absichtlich oder versehentlich zu verändern oder zu zerstören. Die eigenen Daten eines Benutzers sind vor dem Zugriff anderer Benutzer geschützt und können von diesen nicht eingesehen oder verändert werden. Jeder Benutzer kann außerdem seine eigene Arbeitsumgebung einrichten, die er bei jeder neuen Anmeldung am Linux-System unverändert wieder vorfindet.

Sie legen ein solches Benutzerkonto mit dem unter Abb. 1.23 auf der nächs-

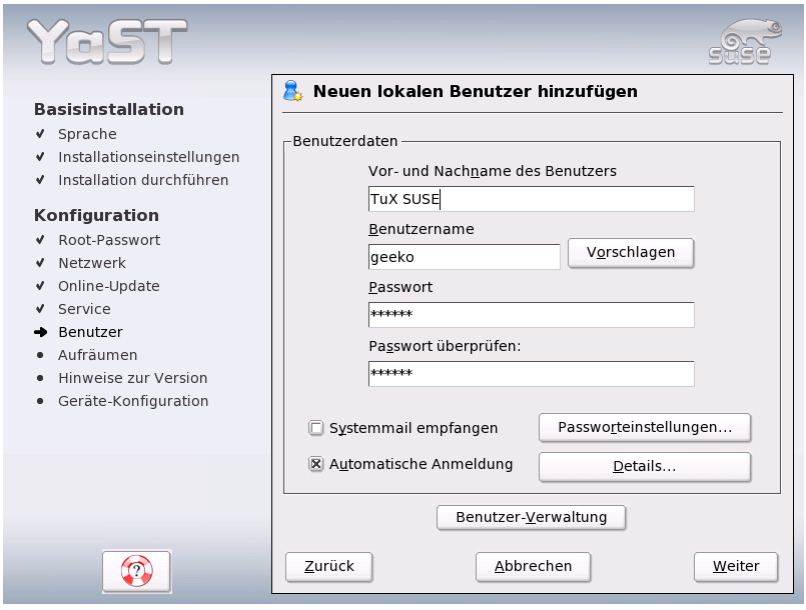

Abbildung 1.23: *Benutzernamen und Passwort angeben*

ten Seite dargestellten Dialog an. Geben Sie Ihren Vor- und Nachnamen ein. Des Weiteren müssen Sie einen Benutzernamen (Loginnamen) wählen. Falls Ihnen kein geeigneter Benutzername einfällt, können Sie sich über den Button 'Vorschlagen' einen Loginnamen automatisch erstellen lassen.

Schließlich ist für den Benutzer noch ein Passwort einzugeben, das zur Vermeidung von Tippfehlern wiederholt werden muss.

Ein Passwort sollte für einen wirkungsvollen Schutz zwischen 5 und 8 Zeichen lang sein. Die maximale Länge eines Passwortes sind 128 Zeichen. Wenn keine speziellen Module geladen sind, werden aber nur die ersten 8 Zeichen zur Passwortunterscheidung genutzt. Groß- und Kleinschreibung wird bei der Passwortvergabe berücksichtigt. Umlaute sind nicht erlaubt, Sonderzeichen und die Ziffern 0-9 dürfen verwendet werden.

Beim lokalen Benutzer gibt es noch zwei Optionen, die wahlweise aktiviert werden können.

'Systemmail empfangen' Wenn Sie diese Checkbox ankreuzen, erhalten Sie Meldungen der Systemdienste. Nomalerweise werden diese nur

an den Administrator `root` gesendet. Weil Sie jedoch nur in Ausnahmefällen als `root` angemeldet sein sollten, macht dies vor allem bei jenem Benutzer Sinn, der hauptsächlich mit dem System arbeitet.

'Automatische Anmeldung' Diese Option ist nur verfügbar, wenn Sie KDE als Desktop verwenden. Sie bewirkt, dass der aktuelle Benutzer nach dem Systemstart automatisch angemeldet wird. Dies ist hauptsächlich dann sinnvoll, wenn der Computer nur von einer einzigen Person genutzt wird. 'Automatische Anmeldung' muss explizit aktiviert werden.

Achtung

Automatische Anmeldung

Bei der automatischen Anmeldung findet nach dem Systemstart keine Authentifizierung statt. Verwenden Sie diese Option *nicht* für Computer, die vertrauliche Daten enthalten und für andere Personen zugänglich sind.

Achtung

1.8.9 Release-Notes lesen

Nach der Konfiguration der Benutzer-Authentifizierung werden die Release-Notes angezeigt. Sie sollten sich in jedem Fall die Zeit nehmen, die Release-Notes zu lesen, denn sie enthalten aktuelle Informationen, die zum Zeitpunkt der Drucklegung der Handbücher noch nicht verfügbar waren. Wenn Sie einen Internet-Zugang eingerichtet und diesen mit dem SUSE-Server getestet haben, wurde dabei ggf. die neueste Version von SUSE geholt, und die Informationen sind auf dem allerneuesten Stand.

1.9 Hardware-Konfiguration

Zum Abschluss der Installation präsentiert YaST noch einen Dialog, in dem Sie die die Möglichkeit haben, die Grafikkarte sowie verschiedene am System angeschlossene Hardware-Komponenten einzurichten. Durch Klicken auf die einzelnen Komponenten können Sie die Hardware-Konfiguration starten. YaST erkennt und konfiguriert die Hardware dann weitgehend automatisch.

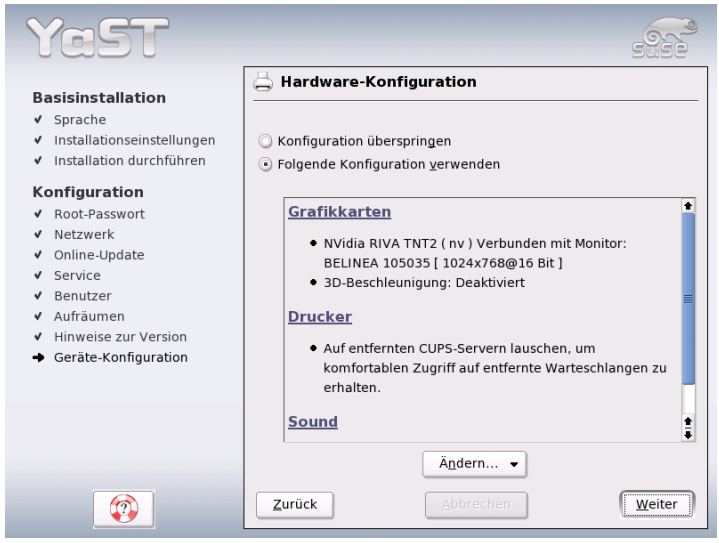

Abbildung 1.24: *Konfiguration der Systemkomponenten*

Hinweis

S/390, zSeries: Hardware-Konfiguration

Auf IBM S/390 und zSeries existiert kein Display, das von XFree unterstützt wird. Der Menüpunkt ‘Grafikkarten’ entfällt auf diesem System.

Hinweis

Die Konfiguration externer Geräte können Sie auch später im installierten System vornehmen, wir empfehlen jedoch, zumindest die Grafikkarte auf die von Ihnen gewünschten Werte einzustellen. Der von YaST ermittelte Standardvorschlag ist zwar in den meisten Fallen zufriedenstellend, jedoch sind gerade bei der Bildschirmdarstellung (Auflösung, Farbtiefe) die Vorlieben von Anwender zu Anwender sehr unterschiedlich. Wenn Sie die Einstellungen ändern wollen, wählen Sie bitte den Punkt ‘Grafikkarten’. Die Bedienung dieses Dialogs ist im Abschnitt 2.4.5 auf Seite 81 beschrieben.

Nachdem YaST die Konfigurationsdaten geschrieben hat, können Sie im Abschluss-Dialog mit ‘Beenden’ die Installation von SUSE LINUX endgültig abschließen.

1.10 Grafisches Login

Hinweis

S/390, zSeries: Grafisches Login

Auf IBM S/390 und zSeries existiert kein grafisches Login.

Hinweis

SUSE LINUX ist nun installiert. Wenn Sie bei lokaler Benutzerverwaltung die automatische Anmeldung aktiviert haben, können Sie ohne Login-Prozedur gleich loslegen. Andernfalls erscheint auf Ihrem Monitor das grafische Login, das Sie in Abb. 1.25 sehen können. Geben Sie bitte den vorher festgelegten Benutzernamen und das dazu gehörige Passwort ein, um sich am System anzumelden.

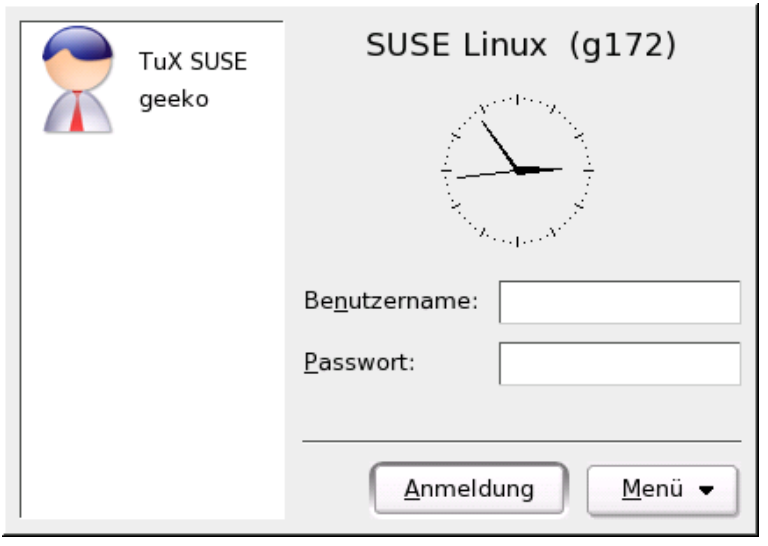

Abbildung 1.25: *Einloggen in das System*

YaST – Konfigurationen

Im SUSE LINUX Enterprise Server übernimmt YaST neben der Installation Ihres Systems auch dessen Konfiguration. Dieses Kapitel behandelt die Konfiguration des wesentlichen Systemkomponenten wie Hardware, Netzwerkzugang, Sicherheitseinstellungen und Benutzerverwaltung. Ausserdem finden Sie am Ende des Kapitels eine Kurzeinführung in die Benutzung des textbasierten YaST.

2.1 Der Start von YaST 52
2.2 Das YaST-Kontrollzentrum 53
2.3 Software 53
2.4 Hardware 73
2.5 Netzwerkgeräte 98
2.6 Netzwerk-Dienste 98
2.7 Sicherheit und Benutzer 103
2.8 System 109
2.9 Sonstiges 117
2.10 YaST im Textmodus (ncurses) 119

2.1 Der Start von YaST

Die Systemkonfiguration mit YaST erfolgt mittels verschiedener YaST-Module, die jeweils einem bestimmten Zweck dienen. Je nach verwendeter Hardwareplattform und installiertem Softwareumfang haben Sie über unterschiedliche Zugangsmöglichkeiten zu YaST im installierten System.

2.1.1 Start über eine grafische Oberfläche

Setzen Sie eine der beiden grafischen Benutzeroberflächen KDE oder GNOME ein, starten Sie das YaST Kontrollzentrum über das SUSE Menü ('SUSE (Menü)' → 'System' → 'YaST'). KDE integriert die einzelnen YaST Konfigurationsmodule zusätzlich in das KDE-Kontrollzentrum.

Bevor YaST startet, wird das Root-Passwort abgefragt, da YaST die Rechte des Systemadministrators benötigt, um die Systemdateien zu ändern.

Sowohl KDE als auch GNOME unterstützen den Start von YaST über die Tastenkombination (Alt) (F2), gefolgt von der Eingabe von `kdesu /sbin/yast2` für KDE oder `gnomesu /sbin/yast2` für GNOME ins Eingabefeld des Befehlsfensters. In beiden Fällen wird anschließend das Root-Passwort abgefragt, bevor YaST startet.

Von der Kommandozeile aus starten Sie YaST über die Befehlsfolge `sux` (Wechsel zum Benutzer `root`) und `yast2`. Möchten Sie die Textversion von YaST starten, geben Sie `yast`anstelle von `yast2` ein,

2.1.2 Start über ein entferntes Terminal

Diese Methode eignet sich für alle Hardwareplattformen, die kein eigenes Display unterstützen, wie z.B. IBM S/390 und zSeries. Sie kann allerdings auch zur Fernwartung von Systemen von einem anderen Rechner aus eingesetzt werden.

1. Öffnen Sie lokal eine Konsole.
2. Geben Sie am Prompt den folgenden Befehl ein, um sich als Benutzer `root` am entfernten System anzumelden und die Ausgabe des X-Servers auf Ihr Terminal umzuleiten:

   ```
   ssh -X root@<Name des Systems>
   ```

3. Sobald das ssh-Login erfolgt ist, geben Sie an Prompt des entfernten Systems `yast2`, um den grafischen Modus von YaST zu starten und auf das lokale Terminal auszugeben. Um YaST im Textmodus zu starten, verwenden Sie `ssh` ohne die Option `-X` und starten YaST mit dem Kommando `yast`.

2.2 Das YaST-Kontrollzentrum

Wenn Sie YaST im grafischen Modus starten, erscheint zunächst das YaST Kontrollzentrum (Abb. 2.1 auf der nächsten Seite). Im linken Bereich finden Sie die Einteilung 'Software', 'Hardware', 'Netzwerkgeräte', 'Netzwerkdienste', 'Sicherheit & Benutzer', 'System' und 'Sonstiges'. Wenn Sie auf eines der Icons klicken, werden rechts die entsprechenden Inhalte aufgelistet. Wenn Sie z. B. 'Hardware' anwählen und dann rechts auf 'Sound' klicken, öffnet sich ein Fenster, in dem Sie die Soundkarte konfigurieren können. Die Konfiguration der einzelnen Punkte erfolgt dabei meist in mehreren Schritten, die Sie jeweils mit 'Weiter' absolvieren können.

Im linken Bildschirmteil wird ein Hilfetext zum jeweiligen Thema angezeigt, der die nötigen Eingaben erklärt. Wenn die erforderlichen Angaben gemacht sind, schließen Sie im jeweils letzten Konfigurationsdialog den Vorgang mit 'Beenden' ab. Die Konfiguration wird dann gespeichert.

2.3 Software

2.3.1 Installationsquelle wechseln

Die Installationsquelle ist das Medium, auf dem die zu installierende Software zur Verfügung steht. YaST kann eine ganze Reihe solcher Quellen verwalten und erlaubt deren gezielte Auswahl für Installation oder Update. Hier können Sie zum Beispiel das SUSE Software Development Kit als Installationsquelle angeben.

Nach dem Start des Moduls wird eine Liste angezeigt, die alle bisher registrierten Quellen enthält. Nach einer normalen CD-Installation ist dort üblicherweise nur die Installations-CD gelistet. Mit 'Hinzufügen' können Sie aber weitere Quellen in diese Liste aufnehmen, wobei nicht nur Wechselmedien wie CDs möglich sind, sondern auch Netzwerk-Verbindungen wie NFS und FTP. Sogar Verzeichnisse auf der lokalen Festplatte können

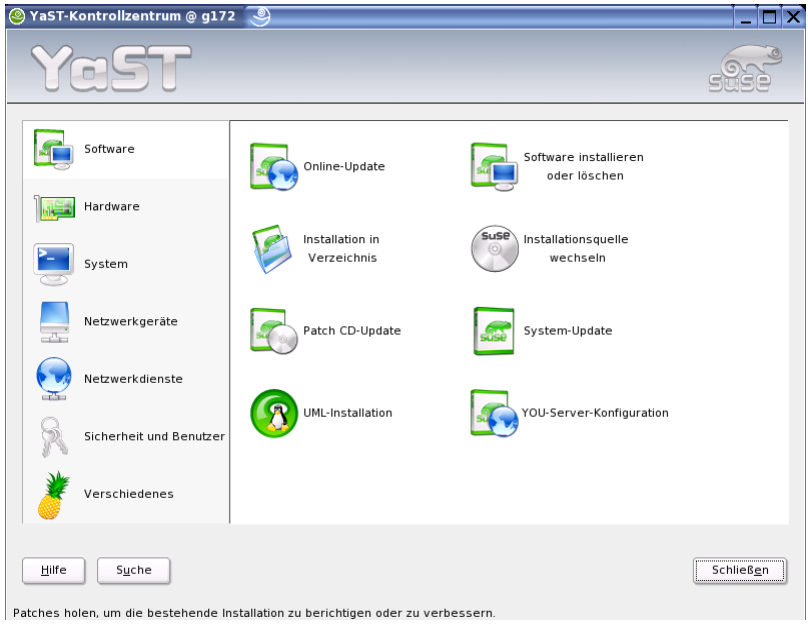

Abbildung 2.1: *Das YaST-Kontrollzentrum*

als Installationsmedium verwendet werden (Lesen Sie bitte den ausführlichen YaST-Hilfetext).

YaST kann bei der Installation oder bei einem Update mehrere Installationsquellen berücksichtigen. Deshalb haben alle hier registrierten Quellen einen Aktivierungszustand, der in der ersten Spalte der Liste angegeben ist. Mit ‘Aktivieren oder Deaktivieren’ können Sie einzelne Quellen ein- oder ausschalten. Bei der Installation von Software-Paketen oder bei einem Update sucht YaST dann aus allen aktivierten Installationsquellen die Passende aus.

Wenn Sie das Modul mit ‘Schließen’ verlassen, werden die aktuellen Einstellungen gespeichert und gelten dann für die Konfigurationsmodule ‘Software installieren oder löschen’ und ‘System-Update’.

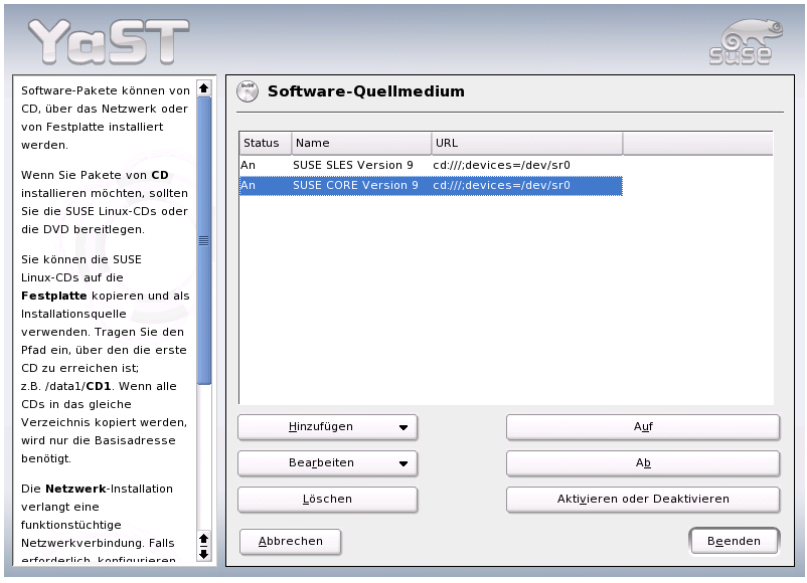

Abbildung 2.2: *Installationsquelle wechseln*

2.3.2 YaST-Online-Update

Das YaST-Online-Update (YOU) ermöglicht die Installation von wichtigen Updates und Verbesserungen. Auf dem SUSE Maintenance Web liegen die aktuellen Patches für Ihr SUSE Produkt zum Herunterladen bereit.

Über das Auswahlfeld ‘Installationsquelle’ können Sie zwischen verschiedenen Servern wählen. Wenn Sie dort einen Server auswählen, wird die zugehörige URL in das Eingabefeld darunter kopiert und kann dort noch editiert werden. Sie können hier auch lokale URLs im Stil von „file:/mein/pfad“ (oder auch nur `/mein/pfad`) angeben. Die bereits vorhandene Liste kann mit ‘Neuer Server’ um zusätzliche Server erweitert werden. Mit ‘Server editieren’ lassen sich die Einstellungen des aktuell gewählten Servers ändern.

Hinweis

Lokaler Updateserver vorhanden

Haben Sie innerhalb Ihres lokalen Netzes mit dem 'YOU-Server' Modul einen eigenen YOU-Server eingerichtet (siehe Abschnitt 4.2 auf Seite 170), können Sie die YOU-Clients im Netz so konfigurieren, dass diese, statt einen Server im Internet anzufragen, Ihren lokalen Server nach Updates anfragen. Die Konfiguration der Clients lesen Sie in Abschnitt 4.2.2 auf Seite 172 nach.

Hinweis

Die Option 'Manuelle Auswahl von Patches' ist beim Start des Moduls aktiviert, damit Sie für jeden einzelnen Patch bestimmen können, ob er geladen werden soll oder nicht. Wollen Sie unbesehen alle verfügbaren Update-Pakete anwenden, dann deaktivieren Sie bitte diese Option. Dies kann aber je nach Bandbreite der Verbindung und der zu übertragenden Datenmenge zu langen Ladezeiten führen.

Wenn Sie die Checkbox 'Alle Patches vom Server neu laden' aktivieren, werden *alle* verfügbaren Patches, installierbare Pakete und Beschreibungen vom Server geholt. Ist diese Box nicht aktiviert (Standard), erhalten Sie nur jene Patches, die noch nicht auf Ihrem System installiert sind.

Zusätzlich gibt es eine Möglichkeit, Ihr System automatisch immer auf dem neuesten Stand zu halten. Mit 'Vollautomatisches Update konfigurieren' kann ein Prozess eingerichtet werden, der regelmäßig selbstständig nach neuen Updates sucht und diese ggf. anwendet. Dieser Vorgang läuft dann vollautomatisch ab, ohne dass Sie irgend etwas dafür tun müssen. Damit dies funktionieren kann, muss natürlich zum gegebenen Zeitpunkt eine Verbindung zum Update-Server hergestellt werden können (z. B. Internet-Verbindung).

Beim manuellen Update (Voreinstellung) wird nach einem Klick auf 'Weiter' eine Liste aller verfügbaren Patches geladen und anschließend der Paket-Manager (s. Abschnitt 2.3.4 auf Seite 59) gestartet. Dort ist dann automatisch der Filter für YOU-Patches aktiviert, und Sie können auswählen, welche Updates installiert werden sollen. Einige der verfügbaren Patches sind i.d.R. beim Start schon angewählt, weil deren Anwendung i.A. sinnvoll ist. Diesen Vorschlag sollten Sie normalerweise übernehmen.

Wenn Sie Ihre Auswahl getroffen haben, klicken Sie im Paket-Manager auf 'Akzeptieren'. Es werden dann alle gewählten Updates vom Server heruntergeladen und anschließend auf Ihrem Rechner installiert. Beides kann je nach Verbindungsqualität und Rechenleistung eine Weile dauern. Falls

dabei Fehler auftreten, werden diese in einem Fenster angezeigt und Sie können das entsprechende Paket ggf. überspringen. Manche Patches öffnen vor der Installation noch ein Fenster zur Darstellung von Detailinformationen. Sie haben dann meist die Wahl, ob Sie das Paket wirklich installieren oder überspringen wollen.

Während die Updates geladen und installiert werden, können Sie im Protokollfenster alle Aktionen verfolgen. Nach der erfolgreichen Installation aller Patches verlassen Sie mit 'Beenden' den YOU-Dialog. Falls Sie die geladenen Update-Dateien nach der Installation nicht noch anderweitig verwenden wollen, sollten Sie mit 'Quellpakete nach dem Update entfernen' die Löschung dieser Dateien veranlassen. Abschließend wird noch das Programm SuSEconfig ausgeführt, um die Konfiguration Ihres Systems den neuen Gegebenheiten anzupassen.

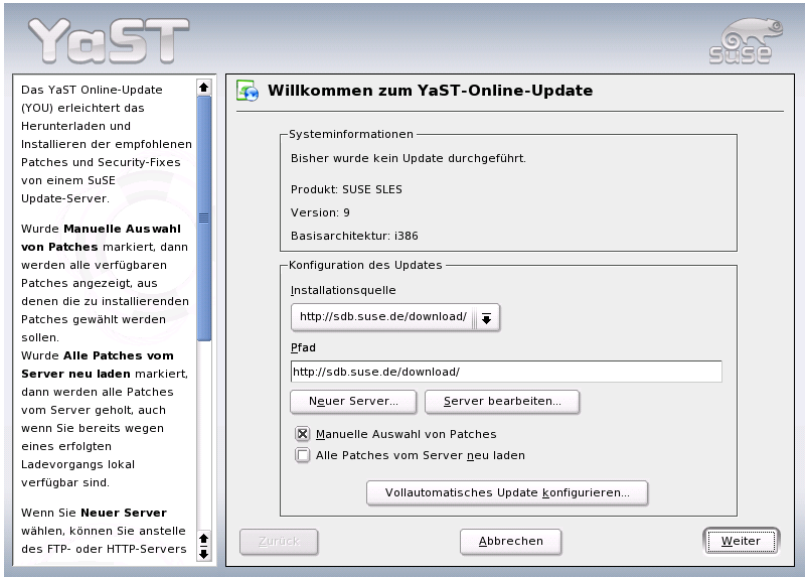

Abbildung 2.3: *YaST: Online-Update*

Zusätzlich zur üblichen Bedienung über die YaST-Oberfläche können Experten das YaST Online Update auch von der Kommandozeile eines Konsolfensters aufrufen. In diesem Fall werden die gewünschten Aktionen durch Kommandozeilen-Parameter wie folgt angegeben: `online_update [Kommandozeilenparameter]`. Die möglichen Parameter werden in der

nachfolgenden Liste zusammen mit ihrer Bedeutung dargestellt.

`-u URL` Basis-URL des Verzeichnisbaumes, aus dem die Patches geladen werden sollen.

`-g` Patches nur herunterladen, jedoch nicht installieren.

`-i` Bereits geladene Patches installieren, jedoch nichts herunterladen.

`-k` Prüfen, ob neue Patches vorhanden sind.

`-c` Aktuelle Konfiguration anzeigen, sonst nichts weiter tun.

`-p Produkt` Produkt, für das Patches geholt werden sollen.

`-v Version` Produktversion, für die Patches geholt werden sollen.

`-a Architektur` Basisarchitektur des Produktes, für das Patches geholt werden sollen.

`-d` „Trockenlauf“ (dry run). Patches holen und Installation simulieren. (System bleibt unverändert, für Testzwecke).

`-n` Keine Signaturprüfung der heruntergeladenen Dateien.

`-s` Liste der verfügbaren Patches anzeigen.

`-V` Verbose-Modus. Gibt Ablaufmeldungen aus.

`-D` Debug-Modus für Experten und zur Fehlersuche.

2.3.3 Patch-CD-Update

Im Gegensatz zum Online-Update werden hier die Patches nicht vom FTP-Server geholt, sondern von CD eingespielt. Der Vorteil ist, dass das Update mit der CD viel schneller geht. Wenn die Patch-CD eingelegt ist, werden im Dialog dieses YaST-Moduls alle Patches, die sich auf der CD befinden, eingelesen und angezeigt. Aus der Patch-Liste können Sie auswählen, welche Pakete installiert werden sollen. Falls Sie vergessen haben sollten, die CD in das Laufwerk zu legen, erscheint eine entsprechende Meldung. Legen Sie dann die CD ein und starten Sie das Patch-CD-Update neu.

2.3.4 Software installieren oder löschen

Mit diesem Modul können Sie Software auf Ihrem Rechner installieren, deinstallieren und aktualisieren. Unter Linux ist Software in Form von Paketen verfügbar. Ein Paket enthält normalerweise alles, was zu einem bestimmten Programm (zum Beispiel ein Editor, ein Compiler usw.) gehört. Dies umfasst i. d. R. das Programm selbst, zugehörige Konfigurationsdateien und eine entsprechende Dokumentation. Weil unter Linux die Quelldateien eines Programmes üblicherweise auch verfügbar sind, gibt es meist ein zugehöriges Paket mit diesen Programmquellen. Die Quellen werden zum Betrieb eines Programmes zwar nicht benötigt, jedoch kann deren Installation sinnvoll sein, wenn man aus bestimmten Gründen eine individuelle, angepasste Version des Programmes erzeugen möchte.

Einige Pakete haben eine funktionale Abhängigkeit zu anderen Paketen. Dies bedeutet, dass die Software eines Paketes nur dann zufriedenstellend funktionieren kann, wenn gleichzeitig auch ein anderes Paket installiert ist (Paket-Abhängigkeit). Darüber hinaus müssen bei manchen Paketen schon für die Installation (also nicht erst zum Betrieb) gewisse andere Pakete installiert sein, zum Beispiel weil die Installationsroutine Gebrauch von bestimmten Tools machen möchte. Wenn solche Pakete installiert werden sollen, muss daher auch noch eine gegebene Reihenfolge beachtet werden. Weiterhin gibt es für manchen Zweck auch mehrere Pakete, die Gleiches oder Ähnliches leisten. Wenn solche Pakete dieselbe Systemressource verwenden, dürfen sie natürlich nicht gleichzeitig installiert werden (Paket-Konflikt). Abhängigkeiten und Konflikte können dabei nicht nur zwischen zwei Paketen existieren, sondern lange Ketten bilden, die in pathologischen Fällen recht unüberschaubar sind. Erschwerend kommt hinzu, dass oft auch die jeweilige Version der Pakete für eine reibungslose Zusammenarbeit entscheidend ist.

All diese Bedingungen müssen beim Installieren, Deinstallieren und Aktualisieren von Software berücksichtigt werden. YaST enthält ein eigenes Software-Installationsmodul; im Folgenden Paket-Manager genannt. Der Paket-Manager verschafft sich beim Start ein aktuelles Bild vom System und kennt daher die bereits installierten Pakete und zeigt sie an. Wenn Sie nun aus der angebotenen Paketvielfalt weitere Pakete zur Installation auswählen, verfolgt der Paket-Manager automatisch (oder auf Anfrage) die o. g. Abhängigkeiten und selektiert ggf. ebenso automatisch weitere Pakete dazu (Auflösung von Abhängigkeiten). Auch wenn Sie versehentlich konkurrierende Pakete auswählen, weist Sie der Paket-Manager auf diesen Umstand hin, und bietet gleichzeitig Vorschläge an, um das Problem zu lösen (Auflösung von Konflikten). Wenn Sie versehentlich ein Paket zum Löschen auswählen, das von anderen bereits installierten Paketen benötigt

wird, erhalten Sie auch hier einen entsprechenden Hinweis mit Detailinformationen und Lösungsvorschlägen.

Über diese rein technischen Aspekte hinaus bietet der Paket-Manager eine übersichtliche Darstellung der Paketfülle in SUSE LINUX. Erreicht wird dies durch thematische Gruppierung der Pakete und eine sinnvoll reduzierte Darstellung dieser Gruppen mittels geeigneter Filter.

Der Paket-Manager

Wenn Sie mit dem Paket-Manager den Software-Bestand auf Ihrem System ändern wollen, wählen Sie bitte im YaST-Kontrollzentrum 'Software installieren oder löschen'. Es erscheint dann das Dialogfenster des Paket-Managers (vgl. Abb. 2.4).

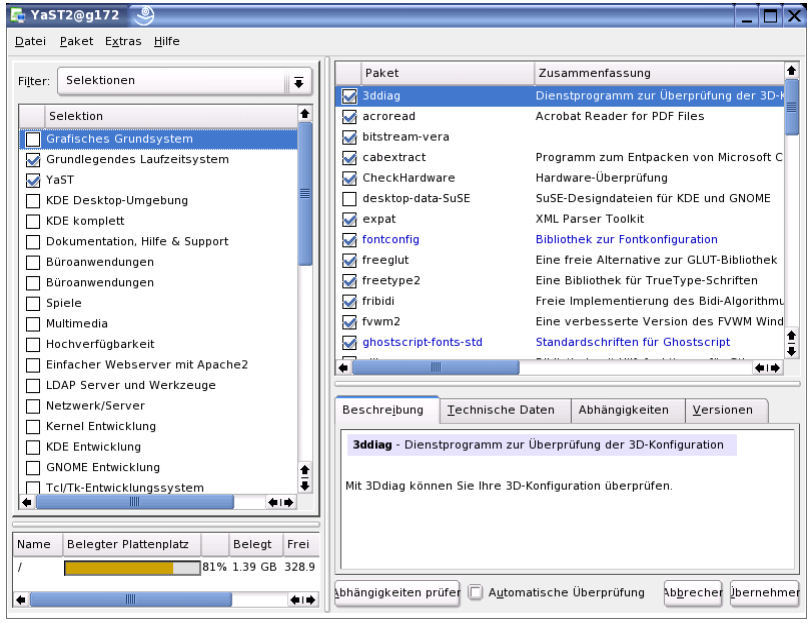

Abbildung 2.4: *YaST: Der Paket-Manager*

Das Fenster ist in verschiedene thematische Bereiche (Teilfenster) aufgeteilt. Die Größen dieser Bereiche sind beim Start nach Erfahrungswerten sinnvoll gewählt. Sie können jedoch verändert werden, wenn Sie die Trennlinien zwischen den Bereichen mit der Maus anklicken und verschieben.

Die Inhalte der Teilbereiche und deren Verwendung werden nachfolgend beschrieben.

Das Filterfenster

Wenn man alle Pakete einer Installation einzeln auswählen wollte, wäre dies ein sehr mühsames und zeitraubendes Unterfangen. Der Paket-Manager bietet deshalb verschiedene Filtermethoden an, die eine zweckdienliche Kategorisierung der Pakete erlauben und einen sinnvoll eingeschränkten Ausschnitt aus der Menge aller Pakete darstellen. Das Filterfenster ist der Bereich links unter der Menüzeile und dient der Steuerung und Darstellung der verschiedenen Filtermethoden. Oben sehen Sie die Filter-Auswahlbox, deren Inhalt bestimmt, was im unteren Teil des Filterfensters dargestellt wird. Wenn Sie die Filter-Auswahlbox aufklappen, sehen Sie eine Liste der vorhandenen Filter und können einen davon verwenden.

Der Selektionen-Filter Beim Start des Paket-Managers ist der so genannte 'Selektionen'-Filter aktiviert. Selektionen gruppieren die Programmpakete nach Anwendungszweck, zum Beispiel „Multimedia“ oder „Büroanwendungen“. Unter der Filter-Auswahlbox sehen Sie die verschiedenen Gruppen des Selektionen-Filters, von denen jene schon ausgewählt sind, die auf Ihrem System bereits installiert sind. Mit einem Mausklick auf die Status-Box am Anfang der Zeile können Sie die Zustände einer Selektion der Reihe nach durchschalten. Alternativ kann der Status auch direkt ausgewählt werden, wenn mit einem rechten Mausklick auf die Zeile einer Selektion das Kontext-Menü aufgeblendet wird. Das Einzelpaketfenster rechts daneben zeigt dabei jeweils eine Liste jener Pakete, die in der aktuellen Selektion enthalten sind. Dort können Sie einzelne Pakete abwählen und natürlich auch wieder anwählen.

Der Paketgruppen-Filter Alternativ kann der 'Paketgruppen'-Filter ausgewählt werden. Dieser Filter erzeugt eine eher technische Sicht auf die Paketmenge und ist gut geeignet für Anwender, die sich in der Paket-Landschaft von SUSE LINUX schon ein wenig auskennen. Die Programmpakete werden hier auf der linken Seite in einer Baumstruktur nach Themen wie „Applikationen“, „Entwicklung“, „Hardware“ usw. geordnet. Je weiter Sie diesen Baum in die Tiefe hinein aufklappen, desto schärfer ist die Eingrenzung der Auswahl auf ein bestimmtes Thema. Die Liste der zugehörigen Pakete rechts im Einzelpaketfenster wird dadurch immer kürzer und überschaubarer.

Zusätzlich bietet dieser Filter die Möglichkeit, *alle* Pakete ohne jede Kategorisierung in alphabetischer Reihenfolge anzuzeigen. Wählen Sie hierzu auf der obersten Ebene den Zweig 'zzz Alle'. Da SUSE LINUX sehr viele Pakete enthält, kann es hier jedoch abhängig von der Hardware-Leistung eine Weile dauern, bis diese lange Liste aufgebaut ist.

Die Suche Die einfachste Methode, ein ganz bestimmtes Paket zu finden, stellt die 'Suche' dar. Durch Angabe verschiedener Suchkriterien können Sie hier oft die Filterung so stark einschränken, dass im Einzelpaketfenster tatsächlich nur ein einziges Paket gelistet wird. Geben Sie hierzu eine Zeichenkette ein, und wählen Sie über die Checkboxen, wie danach gesucht werden soll, also etwa nur im Namen oder auch in der Beschreibung oder in den Paket-Abhängigkeiten. Experten können hier sogar mit Platzhaltern und regulären Ausdrücken spezielle Suchmuster eingeben und in den „Provides"- und „Requires"-Feldern gezielt die Paket-Abhängigkeiten durchsuchen. Software-Entwickler, die Quellpakete aus dem Internet laden, können damit zum Beispiel feststellen, in welchem Paket eine bestimmte Bibliothek enthalten ist, die gebraucht wird, um dieses Paket zu compilieren und zu linken.

Hinweis

Erweiterte Suche im Paket-Manager

Zusätzlich zum 'Suche'-Filter gibt es in allen Listen des Paket-Managers eine Schnellsuche im aktuellen Listeninhalt. Hierzu müssen Sie zum Beispiel nur den Anfangsbuchstaben eines Paketnamens eingeben, und der Cursor springt zum ersten Paket in der Liste, dessen Name mit diesem Zeichen beginnt. Der Cursor muss dabei nur in der Liste stehen (anklicken).

Hinweis

Zusammenfassung der Installation

Nachdem Sie Pakete für die Installation, für ein Update oder zum Löschen ausgewählt haben, sollten Sie sich über die Filter-Auswahlbox eine Installationszusammenfassung anzeigen lassen. Sie sehen dort genau, was mit welchen Paketen geschehen wird, wenn Sie auf 'Akzeptieren' klicken. Über die Reihe von Checkboxen auf der linken Seite können Sie filtern, welche Pakete Sie im Einzelpaketfenster zu sehen wünschen. Wenn Sie zum Beispiel nur überprüfen wollen,

welche Pakete bereits installiert sind, deaktivieren Sie gleich nach dem Start des Paket-Managers alle Checkboxen bis auf ‘Behalten’.

Der Status der Pakete im Einzelpaketfenster kann selbstverständlich auf die übliche Weise geändert werden. Dies kann in Einzelfällen dazu führen, dass ein Paket die Suchkriterien nicht mehr erfüllt. Wenn Sie solche Pakete anschließend aus der Liste entfernen wollen, können Sie die Liste mit ‘Liste aktualisieren’ neu erzeugen lassen.

Das Einzelpaketfenster

Wie bereits oben erwähnt, wird auf der rechten Seite im Einzelpaketfenster eine Liste von einzelnen Paketen dargestellt. Der Inhalt dieser Liste wird immer durch den aktuell ausgewählten Filter bestimmt. Wenn zum Beispiel im Filterfenster der Selektionen-Filter ausgewählt ist, zeigt das Einzelpaketfenster alle Pakete der aktuellen Selektion.

Jedes Paket hat im Paket-Manager einen logischen Zustand, der bestimmt, was mit dem Paket geschehen soll, zum Beispiel „Installieren“ oder „Deinstallieren“. Dieser Zustand wird, ähnlich wie beim Selektionen-Filter, am Anfang der Zeile in einer Status-Box symbolisch dargestellt. Auch hier können Sie mit einem Mausklick den jeweiligen Status der Reihe nach durchschalten oder mit dem Kontext-Menü der rechten Maustaste direkt auswählen. Es gibt eine ganze Reihe von möglichen Zuständen, die aber abhängig von der aktuellen Gesamtsituation nicht immer alle wählbar sind. Es ist zum Beispiel nicht möglich, ein noch nicht installiertes Paket auf „Deinstallieren“ zu setzen. Welche Zustände es gibt, und welche Symbole jeweils dazu gehören, sehen Sie sich am besten direkt im ‘Hilfe’-Menü unter ‘Symbole’ an.

Der Paket-Manager besitzt die folgenden Paketzustände:

Nicht installieren Dieses Paket ist nicht installiert und wird auch nicht installiert.

Installieren Dieses Paket ist noch nicht installiert, wird aber installiert.

Behalten Dieses Paket ist bereits installiert und bleibt unverändert.

Aktualisieren Dieses Paket ist bereits installiert und wird durch die Version vom Installationsmedium ersetzt.

Löschen Dieses Paket ist bereits installiert und wird gelöscht.

Tabu – niemals installieren Dieses Paket ist nicht installiert und wird unter keinen Umständen installiert. Es wird so behandelt, als existierte es auf keinem der Installationsmedien. Wenn ein Paket zur Auflösung von Abhängigkeiten eigentlich automatisch dazu gewählt würde, kann dies mit „Tabu“ verhindert werden. Dadurch können sich jedoch Inkonsistenzen ergeben, die manuell aufgelöst werden müssen (Konsistenzprüfung). „Tabu“ ist deshalb hauptsächlich für Experten gedacht, die genau wissen, was sie tun.

Geschützt Dieses Paket ist installiert und soll nicht verändert werden, da unaufgelöste Abhängigkeiten zu anderen Paketen bestehen oder auftreten könnten. Pakete von Drittanbietern (Pakete ohne SUSE-Signatur) bekommen diesen Status automatisch zugewiesen, damit sie nicht von neueren, auf den Installationsmedien vorhandenen Versionen überschrieben werden. Dies kann Paket-Konflikte verursachen, die manuell aufgelöst werden müssen (für Experten).

Automatisch installieren Dieses Paket wurde vom Paket-Manager automatisch zum Installieren ausgewählt, da es für ein anderes Paket erforderlich ist (Auflösung von Paket-Abhängigkeiten).

Hinweis

Um ein solches Paket abzuwählen, müssen Sie möglicherweise den Status „Tabu“ verwenden (siehe dort).

Hinweis

Automatisch aktualisieren Dieses Paket ist bereits installiert. Da es von einem anderen Paket aber in einer neueren Version benötigt wird, wird die installierte Version automatisch aktualisiert.

Automatisch löschen Dieses Paket ist bereits installiert, aber bestehende Paket-Konflikte machen eine Löschung dieses Pakets erforderlich. Das kann zum Beispiel der Fall sein, wenn ein anderes Paket das aktuelle ersetzt. Dieser Fall kommt äußerst selten vor.

Automatisch installieren (nach Auswahl)
Dieses Paket wurde automatisch zur Installation ausgewählt, weil es Bestandteil einer vordefinierten Selektion ist (zum Beispiel „Multimedia“ oder „Entwicklung“).

Automatisch aktualisieren (nach Auswahl)
Dieses Paket ist bereits installiert, aber es existiert eine neuere Version auf den Installationsmedien. Es ist Bestandteil einer vordefinierten

Selektion (zum Beispiel „Multimedia“ oder „Entwicklung“), die Sie zum Update ausgewählt haben und wird automatisch aktualisiert.

Automatisch löschen (nach Auswahl)
Dieses Paket ist bereits installiert, aber eine vordefinierte Selektion (z.B. „Multimedia“ oder „Entwicklung“) macht seine Löschung erforderlich. Dieser Fall kommt nur sehr selten vor.

Zusätzlich können Sie noch bestimmen, ob zu einem Paket die Quellen mit installiert werden sollen oder nicht. Diese Information ergänzt den aktuellen Paket-Zustand und kann deshalb weder mit Mausklick durchgeschaltet werden, noch im Kontext-Menü direkt angewählt werden. Stattdessen gibt es am Ende der Paketzeile eine Checkbox zur Auswahl der Quellen-Pakete. Wenn diese Checkbox in der Liste nicht dargestellt wird, müssen Sie evtl. ganz nach rechts scrollen, um sie sichtbar zu machen. Alternativ finden Sie diese Option im Menü ‘Paket’.

Quellen installieren Der Quellcode wird mit installiert

Quellen nicht installieren Der Quellcode wird nicht installiert.

Zusätzliche Information liefert die Schriftfarbe, die im Einzelpaketfenster für die verschiedenen Pakete verwendet wird. Bereits installierte Pakete, die auf den Installationsmedien in einer neueren Version verfügbar sind, werden blau angezeigt. Installierte Pakete mit einer höheren Versionsnummer als jene auf den Installationsmedien werden rot dargestellt. Weil die Versionsnummerierung von Paketen nicht immer kontinuierlich fortlaufend ist, kann aber nicht in jedem Fall eine eindeutige Beziehung hergestellt werden. Die Information ist daher nicht absolut „wasserdicht“, sollte aber genügen, um einen Hinweis auf problematische Pakete zu geben. Im Infofenster können Sie sich dann die Versionsnummern genauer ansehen.

Das Infofenster

Im Infofenster rechts unten können Sie mittels der Reiter verschiedene Informationen zu dem jeweils ausgewählten Paket nachsehen. Beim Start ist die Beschreibung des aktuellen Pakets aktiviert. Über die verschiedenen Reiter können Sie umschalten auf die technischen Paketdaten (Größe, Paketgruppe usw.), auf die Liste der Abhängigkeiten zu anderen Paketen und auf die Versionsübersicht.

Das Ressourcenfenster

Damit Sie während der Zusammenstellung Ihrer Software-Auswahl immer wissen, wie sich die aktuelle Auswahl auf den freien Festplattenplatz auswirkt, zeigt das Ressourcenfenster links unten die Belegung aller aktuell gemounteten Filesysteme an. Für jedes Filesystem wird die aktuelle Belegung in einem farbigen Balkendiagramm graphisch dargestellt. Grün bedeutet „viel Platz“. Je „enger“ es wird, umso mehr wandelt sich die Balkenfarbe zu Rot. Die dargestellten Werte repräsentieren dabei jene Belegung, die sich ergäbe, wenn Sie die aktuelle Auswahl übernehmen würden. Wenn Sie zu viele Pakete für die Installation auswählen, erscheint zusätzlich noch ein Warnfenster.

Die Menüzeile

Die Menü-Zeile links oben im Fenster erlaubt einen alternativen Zugang zu den meisten der bereits beschriebenen Funktionen und bietet darüber hinaus einige mehr, die auf andere Weise nicht erreicht werden können. Sie enthält vier Menüs:

Datei Unter ‘Datei’ wird über den Menüpunkt ‘Exportieren’ eine Liste aller installierten Pakete in einer Textdatei abgespeichert. Dies ist sinnvoll, wenn Sie einen bestimmten Installationsumfang zu einem späteren Zeitpunkt oder auf einem anderen System exakt nachbilden wollen. Eine derart erzeugte Datei kann dann mit ‘Importieren’ wieder eingelesen werden und erzeugt dabei genau die gleiche Paketauswahl, die beim Abspeichern vorlag. In beiden Fällen können Sie den Speicherort der Datei selbst bestimmen oder den angebotenen Vorschlag übernehmen.

Über den Menüpunkt ‘Beenden – Änderungen verwerfen’ verlassen Sie den Paket-Manager, wobei alle Veränderungen an der Paketauswahl seit dem Start verlorengehen. Wenn Sie Ihre Änderungen speichern wollen, wählen Sie ‘Beenden – Änderungen speichern’. Es werden dann alle Änderungen durchgeführt und das Programm anschließend beendet.

Paket Die Punkte im Menü ‘Paket’ beziehen sich immer auf das aktuelle Paket im Einzelpaketfenster. Sie sehen hier alle Zustände, die ein Paket annehmen kann. Allerdings sind davon nur jene wählbar, die beim aktuellen Paket möglich und sinnvoll sind. Mit den Checkboxen können Sie bestimmen, ob die zum Paket gehörenden Quellen mit installiert werden sollen oder nicht. Der Punkt ‘Alle in dieser Liste’

öffnet ein Untermenü, das nochmals alle diese Paket-Zustände enthält. Eine Auswahl hier betrifft jedoch nicht nur das aktuelle Paket, sondern *alle* Pakete in dieser Liste.

Extras Das Menü 'Extras' bietet Optionen zur Handhabung von Paket-Abhängigkeiten und -Konflikten. Wenn Sie schon manuell Pakete zur Installation ausgewählt haben, erhalten Sie mit 'Automatische Paketänderungen anzeigen' eine Liste jener Pakete, die der Paket-Manager zur Auflösung von Abhängigkeiten automatisch dazu gewählt hat. Wenn zu diesem Zeitpunkt noch unaufgelöste Paket-Konflikte existieren, kommt vorher ein entsprechender Hinweis mit Lösungsvorschlägen.

Wenn Sie Paket-Konflikte auf „Ignorieren" setzen, wird diese Information permanent im System gespeichert. Andernfalls müssten Sie bei jedem Start des Paket-Managers immer wieder die gleichen Pakete auf „Ignorieren" setzen. Für den Fall, dass Sie solche ignorierten Ahängigkeiten wieder zurücksetzen möchten, können Sie dies mit 'Ignorierte Abhängigkeitskonflikte zurücksetzen' wieder rückgängig machen.

Hilfe Unter 'Hilfe' können Sie mit 'Überblick' eine kurze Erklärung der Paket-Manager-Funktionalität anzeigen lassen. Eine genaue Erläuterung der verschiedenen Paket-Zustände mit den zugehörigen Symbolen finden Sie unter 'Symbole'. Falls Sie Programme lieber ohne Verwendung der Maus bedienen, können Sie mit dem Menüpunkt 'Tasten' eine Erläuterung der Tastenkürzel aufrufen.

Konsistenzprüfung

Unterhalb des Infofensters finden Sie den Button 'Konsistenzprüfung' und daneben die Checkbox 'Automatische Überprüfung'. Wenn Sie auf 'Konsistenzprüfung' klicken, überprüft der Paket-Manager, ob sich bei der aktuellen Paketauswahl unaufgelöste Paket-Abhängigkeiten oder -Konflikte ergeben. Bei unaufgelösten Abhängigkeiten werden dann automatisch die zusätzlich zu Ihrer Auswahl benötigten Pakete angewählt, und die Abhängigkeiten auf diese Weise ohne ihr Zutun erfüllt. Bei Paket-Konflikten öffnet der Paket-Manager ein Fenster zur Darstellung des Konflikts und bietet darin auch gleich verschiedene Lösungsmöglichkeiten an.

Wenn Sie die 'Automatische Überprüfung' aktivieren, erfolgt o.g. Prüfung jedes Mal nach der Änderung eines Paket-Status. Dies ist einerseits praktisch, weil so die Konsistenz der Paketauswahl permanent überwacht wird. Andererseits kostet diese Prüfung auch einiges an Rechenleistung und

kann die Bedienung des Paket-Managers träge machen. Aus diesem Grund ist die automatische Prüfung beim Start des Paket-Managers nicht aktiviert. Sie können selbst entscheiden wie es praktischer für Sie ist. In jedem Fall erfolgt eine Konsistenzprüfung, wenn Sie Ihre Auswahl mit 'Akzeptieren' übernehmen.

Im folgenden Beispiel dürfen `sendmail` und `postfix` nicht gleichzeitig installiert werden. In Abbildung 2.5 auf der nächsten Seite sehen Sie die Konfliktmeldung, die nun von Ihnen eine Entscheidung verlangt. `postfix` ist bereits installiert, also können Sie entweder auf die Installation von `sendmail` verzichten, `postfix` entfernen lassen oder das Risiko eingehen und den Konflikt ignorieren.

Achtung

Bearbeitung von Paket-Konflikten

Folgen Sie bei der Bearbeitung von Paket-Konflikten den Vorschlägen des YaST Paket-Managers, da andernfalls die Stabilität und Funktionsfähigkeit Ihres Systems durch den bestehenden Konflikt gefährdet ist.

Achtung

2.3.5 System-Update

Dieses Modul ermöglicht es, Ihr aktuelles System auf einen neueren Versionenstand zu bringen. Im laufenden Betrieb kann damit allerdings nur Applikations-Software erneuert werden, nicht aber das SUSE LINUX- Basissystem. Hierfür muss vom Installationsmedium, zum Beispiel der CD, gebootet werden. Bei der Auswahl des Installationsmodus in YaST wählen Sie dann bitte 'Update des bestehenden Systems' statt 'Neuinstallation'.

Die Vorgehensweise beim Update des Systems ähnelt stark dem Ablauf bei der Neuinstallation. YaST ermittelt zunächst den aktuellen Zustand Ihres Systems, bestimmt eine günstige Update-Strategie und präsentiert dann die Ergebnisse in einem Vorschlags-Dialog (siehe Abb. 2.6 auf Seite 70). Wie schon bei der Installation können Sie auch hier beim Update die einzelnen Punkte mit der Maus anklicken, um detaillierte Änderungen vorzunehmen. Einige dieser Punkte, wie 'Sprache' und 'Tastaturbelegung', wurden schon bei der Installation erklärt (siehe Abschnitt 1.4 auf Seite 13). Im Folgenden werden daher nur Update-spezifische Einstellungen erläutert.

Abbildung 2.5: *Konflikt-Management des Paket-Managers*

Ausgewählt für Update

Falls auf Ihrem System mehrere Versionen von SUSE LINUX installiert sind, können Sie hier auswählen, welche Partition für das Update verwendet werden soll. Alle Partitionen, die für ein Update in Frage kommen, werden hier in einer Liste angezeigt, und Sie können eine davon auswählen.

Update-Optionen

Hier können Sie einstellen, auf welche Weise Ihr System aktualisiert werden soll. Zwei Möglichkeiten stehen zur Auswahl (siehe Abb. 2.7 auf Seite 71).

Update mit Installation neuer Software
: Falls das System komplett auf den neuen Softwarestand gebracht werden soll, kann eine der vordefinierten Selektionen ausgewählt werden. Diese Selektionen sind die gleichen, die auch bei der Installation angeboten werden und sorgen dafür, dass auch neue, bisher nicht vorhandene Pakete installiert werden.

Abbildung 2.6: *Vorschlags-Dialog beim Update*

Nur installierte Pakete aktualisieren
: Mit dieser Option werden nur jene Pakete erneuert, die auf dem aktuellen System schon vorhanden sind. Es werden keine neuen Features installiert.

Zusätzlich können Sie noch mit ‘Nicht gepflegte Pakete löschen’ bestimmen, ob jene Pakete gelöscht werden sollen, die in der neuen Version nicht mehr vorhanden sind. Diese Option ist beim Start angewählt, um zu verhindern, dass veraltete Pakete unnötig Plattenplatz verbrauchen.

Pakete

Mit ‘Pakete’ starten Sie den Paket-Manager und können dort gezielt einzelne Pakete zum Update an- oder abwählen. Auch Paket-Konflikte, die hier vielleicht angezeigt werden, sollten dort mit der Konsistenzprüfung gelöst werden. Die Bedienung des Paket-Managers wird ausführlich im Abschnitt 2.3.4 auf Seite 59 erklärt.

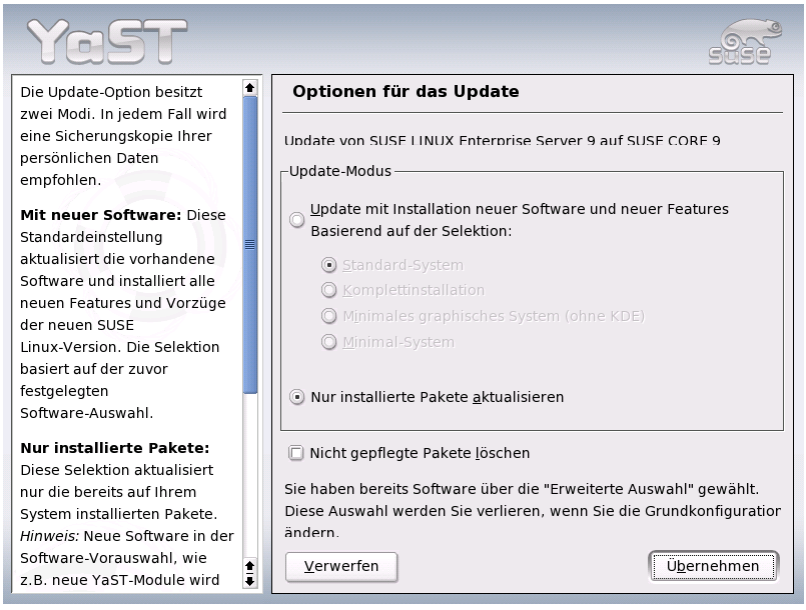

Abbildung 2.7: Update Optionen

Backup

Beim Update werden u.U. die Konfigurationsdateien einzelner Pakete durch jene der neuen Version ersetzt. Weil nicht ausgeschlossen werden kann, dass Sie solche Dateien in Ihrem aktuellen System verändert haben, werden die ersetzten Dateien normalerweise vorher gesichert. In diesem Dialog können Sie bestimmen, ob und in welchem Umfang diese Sicherungen angelegt werden sollen.

Hinweis

Umfang des Backups

Bitte beachten Sie, dass dieses Backup nicht die gesamte Software umfasst, sondern nur die entsprechenden Konfigurationsdateien.

Hinweis

Wichtige Hinweise zum Update

Das Update des Systems ist softwaretechnisch ein hochkomplexes Verfahren. YaST muss dabei für jedes Programmpaket prüfen, welche Version sich

auf dem Rechner befindet und danach, was zu tun ist, damit die neue Version die alte korrekt ersetzt. Dabei muss YaST darauf achten, zu möglichst jedem installierten Paket eventuell vorhandene persönliche Einstellungen soweit als möglich zu übernehmen, damit Sie Ihre eigenen Konfigurationen nicht wieder komplett anpassen müssen.

In den meisten Fällen wird YaST diesen Anforderungen gerecht und ersetzt alte Versionen gegen neue, ohne dass Sie Probleme bemerken. Um sicherzugehen, dass vorhandene Konfigurationen nach einem Update nicht verlorengehen, sollten Sie auf jeden Fall vor dem Update eine Sicherung Ihres bestehenden Systems machen. So können auftretende Konflikte nach dem Update manuell aufgelöst werden.

Hinweis

Hinweise zum System-Update

Dieses Handbuch enthält ein ganzes Kapitel, das sich mit dem Thema Update befasst (siehe Kapitel 5 auf Seite 177). In einem eigenen Abschnitt werden sämtliche wichtigen Änderungen gegenüber der Vorversion erläutert und auf eventuell auftretende Update-Probleme hingewiesen (siehe Abschnitt 5.2.1 auf Seite 184).

Hinweis

2.3.6 SUSE Software Development Kit 9 (SDK)

SUSE Software Development Kit 9 ist ein umfassendes Toolkit zur Applikationsentwicklung für SUSE LINUX Enterprise Server 9 und Novell Linux Desktop. Das SUSE Software Development Kit enthält sämtliche Open-Source Werkzeuge, mit denen das SUSE LINUX Enterprise Server Produkt gebaut wurde. Als Entwickler, Independent Software Vendor (ISV) oder Independent Hardware Vendor (IHV) stehen Ihnen alle Werkzeuge zur Verfügung, die Sie zur Portierung von Anwendungen auf alle von SUSE LINUX Enterprise Server und Novell Linux Desktop unterstützten Plattformen benötigen.

Das SUSE Software Development Kit enthält ausserdem Integrated Development Environments (IDEs), Debugger, Code-Editoren und andere Werkzeuge. Es unterstützt die meisten großen Programmiersprachen (inklusive C, C++, Java und den meisten Skriptsprachen). Es enthält zudem einige zusätzliche Perl-Pakete, die im Softwareumfang des SUSE LINUX Enterprise Server nicht enthalten sind.

Weitere Detailinformationen finden Sie unter `http://developer.novell.com/ndk/susesdk.htm`. Die Softwarepakete des SUSE Software Development Kit 9 werden mit Hilfe des YaST Paketmanagers installiert.

2.4 Hardware

Neue Hardware muss entsprechend den Vorgaben des Herstellers eingebaut bzw. angeschlossen werden. Schalten Sie externe Geräte an und rufen Sie das entsprechende YaST-Modul auf. Ein Großteil der handelsüblichen Geräte wird von YaST automatisch erkannt und die technischen Daten angezeigt. Falls die automatische Erkennung fehlschlägt, bietet YaST eine Geräteliste an (zum Beispiel Modell/Hersteller), aus der Sie das passende Gerät auswählen. Konsultieren Sie die Dokumentation zu Ihrer Hardware, wenn die auf Ihrem Gerät aufgedruckte Information nicht ausreicht.

Hinweis

Modellbezeichnungen

Achtung bei Modellbezeichnungen: Im Zweifelsfall empfiehlt es sich, es mit einer ähnlichen Bezeichnung zu probieren, wenn Sie Ihr Modell in der Geräteliste nicht finden. In manchen Fällen ist jedoch eine absolut buchstaben- bzw. nummerngetreue Angabe unerlässlich, denn ähnliche Bezeichnungen lassen nicht immer auf Kompatibilität schließen.

Hinweis

2.4.1 CD-ROM-Laufwerke

Im Rahmen der Installation werden alle erkannten CD-ROM-Laufwerke in das installierte System eingebunden, d.h. es werden entsprechende Einträge in der Datei `/etc/fstab` vorgenommen und die Unterverzeichnisse in `/media` werden angelegt. Mit diesem YaST-Modul können Sie auch nachträglich eingebaute Laufwerke in das System integrieren.

Nach dem Aufruf des Moduls wird eine Liste mit allen erkannten Laufwerken präsentiert. Markieren Sie Ihr neues Laufwerk in der Checkbox am Zeilenanfang und schließen Sie dann mit 'Beenden' ab. Das neue Laufwerk wird nun ins System integriert und ist verwendbar.

Hinweis

S/390, zSeries: Einbinden von SCSI CD-ROM-Laufwerks

Die Einbindung eines SCSI CD-ROM-Laufwerks in ein IBM S/390 und zSeries System erfordert folgende Vorarbeiten:

- Schließen Sie das Gerät an einen FCP-Adapter an.
- Aktivieren Sie dieses Gerät mit YaST ähnlich der Aktivierung von ZFCP-Platten (siehe Abschnitt 1.5 auf Seite 14).

Das restliche Vorgehen ist wie oben beschrieben.

Hinweis

2.4.2 S/390, zSeries: DASD

Um dem installierten System zusätzliche DASD-Platten hinzuzufügen, verwenden Sie das YaST DASD-Modul ('Hardware' → 'DASD'). Im ersten Dialog wählen Sie die Platten aus, die Sie Ihrem Linux-System zur Verfügung stellen möchten und klicken Sie auf 'Aktion durchführen'. Wählen Sie als 'Aktivieren' als Aktionstyp aus und verlassen Sie diesen Dialog mit 'Weiter'.

Um die ausgewählte/n Platte/n dauerhaft (über den nächsten Reboot hinaus) ins System zu integrieren, fahren Sie wie folgt fort:

- Falls die Verwaltung der DASDs im System über eine Parameterliste in `/etc/zipl.conf` vorgenommen wird (z.B. `dasd=301,302`), ergänzen Sie diese Liste in `/etc/zipl.conf` um die neuen Einträge.
- Andernfalls führen Sie die Befehle `cd /boot` und `mkinitrd` aus. Überprüfen Sie, ob die neuen Einträge in der Ausgabe von `mkinitrd` enthalten sind.

Abschließend rufen Sie `zipl -V` auf, um die neue Konfiguration zu übernehmen.

2.4.3 Drucker

Unter Linux werden Drucker über Druckerwarteschlangen angesprochen. Die zu druckenden Daten werden dabei in der Druckerwarteschlange zwischengespeichert und durch den Druckerspooler nacheinander zum Drucker geschickt.

Meist liegen diese Daten nicht in einer Form vor, die direkt an den Drucker geschickt werden könnte. Eine Grafik muss zum Beispiel normalerweise in ein Format umgewandelt werden, das der Drucker direkt ausgeben kann. Die Umwandlung in die Druckersprache erfolgt durch den Druckerfilter, der vom Druckerspooler zwischengeschaltet wird, um Daten ggf. so umzuwandeln, dass sie der Drucker direkt ausgeben kann.

Hinweis

Weitere Informationen

Tiefergehende Informationen zum Thema *Drucken unter Linux* schlagen Sie im Kapitel 13 auf Seite 323 nach.

Hinweis

Konfiguration mit YaST

Zur Druckereinrichtung wählen Sie im YaST-Kontrollzentrum unter 'Hardware' den Punkt 'Drucker'. Es erscheint das Hauptfenster der Druckereinrichtung. Hier sehen Sie im oberen Fenster die erkannten Drucker, im unteren Fenster die eingerichteten Warteschlangen. Wurde ein Drucker nicht automatisch erkannt, können Sie den Drucker manuell einrichten.

Automatische Konfiguration

YaST ermöglicht eine automatische Konfiguration des Druckers, wenn folgende Bedingungen erfüllt sind:

1. Der parallele bzw. der USB-Anschluss wird automatisch korrekt eingerichtet und der daran angeschlossene Drucker automatisch erkannt.
2. In der Druckerdatenbank findet sich die Identifikation des Druckermodells, die YaST bei der automatischen Hardwareerkennung erhalten hat. Diese Hardware-Identifikation unterscheidet sich bei manchen Druckern von der Modellbezeichnung. In diesem Fall kann das Modell unter Umständen nur manuell ausgewählt werden.

Für jede Konfiguration sollte grundsätzlich mit dem YaST-Testdruck ausprobiert werden, ob sie tatsächlich funktioniert. Die YaST-Testseite liefert zusätzlich wichtige Informationen zur jeweiligen Konfiguration.

Manuelle Konfiguration

Wenn eine der Bedingungen für die automatische Konfiguration nicht erfüllt ist oder eine spezielle individuelle Konfiguration gewünscht wird, muss die Einrichtung manuell erfolgen.

Je nachdem inwieweit YaST die Hardware automatisch erkennt und inwieweit zu dem jeweiligen Druckermodell Informationen in der Druckerdatenbank vorhanden sind, kann YaST die benötigten Daten automatisch ermitteln oder eine sinnvolle Vorauswahl anbieten.

Insgesamt müssen folgende Werte konfiguriert werden:

Hardwareanschluss (Schnittstelle)
Wie der Hardwareanschluss zu konfigurieren ist, hängt davon ab, ob YaST den Drucker bei der Hardware-Erkennung finden konnte.

- Kann YaST das Druckermodell automatisch erkennen, ist davon auszugehen, dass der Druckeranschluss auf Hardwareebene funktioniert und es müssen hier keine Einstellungen vorgenommen werden.
- Kann YaST das Druckermodell nicht automatisch erkennen, deutet dies darauf hin, dass der Druckeranschluss auf Hardware-Ebene nicht ohne manuelle Konfiguration funktioniert.

Name der Warteschlange Da der Warteschlangenname beim Drucken oft eingegeben werden muss, sollten nur kurze Namen aus Kleinbuchstaben und evtl. Zahlen verwendet werden.

Druckermodell und PPD-Datei Die druckerspezifischen Einstellungen (z. B. Ghostscript-Treiber und zugehörige treiberspezifische Parameter für den Druckerfilter) sind in einer PPD-Datei gespeichert. Für viele Druckermodelle stehen mehrere PPD-Dateien zur Verfügung (z. B. wenn mehrere Ghostscript-Treiber funktionieren).

Durch die Wahl von Hersteller und Modell werden somit zunächst nur die passenden PPD-Dateien ausgewählt. Wenn mehrere PPD-Dateien zur Verfügung stehen, wählt YaST aus diesen eine PPD-Datei aus (normalerweise diejenige, die durch den Eintrag recommended gekennzeichnet ist). Bei Bedarf kann via ‘Ändern’ eine andere PPD-Datei gewählt werden.

Da bei Nicht-PostScript-Druckern der Druckerfilter mit einem Ghostscript-Treiber die druckerspezifischen Daten erzeugt, ist die Konfiguration des Ghostscript-Treibers die entscheidende Stelle, an

der die Art des Ausdrucks festgelegt wird. Die Wahl des Ghostscript-Treibers (via PPD-Datei) und entsprechende treiberspezifische Einstellungen bestimmen das Druckbild. Bei Bedarf können via 'Ändern' andere druckerspezifische Einstellungen für den Druckerfilter in der PPD-Datei gewählt werden.

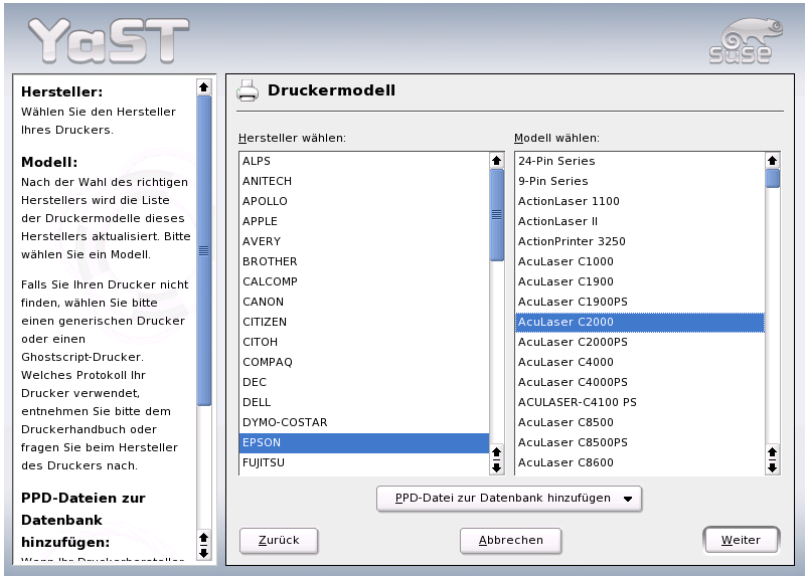

Abbildung 2.8: *YaST2-Druckereinrichtung: Wahl des Druckers*

Ein Drucken der YaST Testseite ist unerlässlich. Wenn beim Drucken der Testseite Unsinn gedruckt wird (zum Beispiel viele fast leere Seiten), können Sie den Druck sofort am Drucker stoppen, indem Sie alles Papier entnehmen und dann den Testdruck abbrechen.

Ist das Druckermodell nicht in der Druckerdatenbank eingetragen, so gibt es eine Auswahl an generischen PPD-Dateien für die Standarddruckersprachen. Wählen Sie dazu als „Hersteller“ UNKNOWN MANUFACTURER.

Weitere Einstellungen Im Normalfall brauchen und sollten Sie keine weiteren Einstellungen vornehmen.

Konfiguration für Anwendungsprogramme

Anwendungsprogramme verwenden die bestehenden Warteschlangen analog zum Drucken auf der Kommandozeile. Konfigurieren Sie daher in den Anwendungsprogrammen im Normalfall nicht den Drucker erneut, sondern verwenden Sie die existierenden Warteschlangen.

Drucken auf der Kommandozeile Auf der Kommandozeile druckt man mit dem Befehl `lp -d` ⟨*`Warteschlange`*⟩ ⟨*`Dateiname`*⟩ wobei ⟨*Warteschlange*⟩ und ⟨*Dateiname*⟩ passend zu ersetzen sind.

Druck via Kommandozeile in Anwendungsprogrammen
Manche Anwendungsprogramme verwenden den `lp`-Befehl zum Drucken. Geben Sie in der Druckmaske des Anwendungsprogramms das passende Druck-Kommando (ohne ⟨*Dateiname*⟩) ein. Zum Beispiel: `lp -d` ⟨*`Warteschlange`*⟩ Der Druckdialog in KDE-Programmen ist dazu aber auf 'Druck über ein externes Programm' umzustellen, weil sonst kein Druckbefehl eingegeben werden kann.

Druck via CUPS-Drucksystem Druckerdialogprogramme wie xpp oder das KDE-Programm kprinter, ermöglichen es, nicht nur die Warteschlange zu wählen, sondern auch CUPS-Standardoptionen und druckerspezifische Optionen aus der PPD-Datei über grafische Auswahlmenüs einzustellen.

Um kprinter in verschiedenen Anwendungsprogrammen als einheitlichen Druckdialog zu bekommen, geben Sie in der Druckmaske der Anwendungsprogramme als Druckbefehl `kprinter` oder `kprinter --stdin` ein. Welcher Druckbefehl zu nehmen ist, hängt vom Anwendungsprogramm ab. Dadurch erscheint nach der Druckmaske des Anwendungsprogramms der kprinter-Druckerdialog, in dem Sie die Warteschlange und die weiteren Optionen einstellen. Bei dieser Methode ist darauf zu achten, dass sich die Einstellungen in der Druckmaske des Anwendungsprogramms und in kprinter nicht widersprechen. Sinnvollerweise nehmen Sie Einstellungen dann nur in kprinter vor.

Mögliche Probleme

Kommt es zu einer Störung in der Kommunikation zwischen Rechner und Drucker, kann der Drucker die gesendeten Daten nicht sinnvoll umsetzen und es werden möglicherweise Unmengen Papier mit „wirren" Zeichen bedruckt; in einem solchen Fall vgl. den Abschnitt 13.7.8 auf Seite 345.

CUPS im Netzwerk konfigurieren

Als Leitfaden zur Konfiguration von „CUPS im Netzwerk“ siehe diesen Grundlagen-Artikel: `http://portal.suse.com/sdb/de/2004/05/jsmeix_print-cups-in-a-nutshell.html`

Bei „CUPS im Netzwerk“ sind die folgenden drei Themenbereiche zu unterscheiden:

1. Konfigurieren Sie auf dem Server die Warteschlangen für die Drucker, die zu dem Server gehören.
2. Erlauben Sie den Zugriff auf die Warteschlangen für die Client-Rechner.
3. Aktivieren Sie das Senden von Browsing-Information an die Client-Rechner.

Bei Punkt 1 müssen die folgenden Fälle unterschieden werden:

Netzwerkdrucker oder Printserver-Box
: via TCP-Socket: mit lokaler Filterung (Default) oder ohne lokale Filterung

  via LPD-Protokoll: mit lokaler Filterung (Default) oder ohne lokale Filterung

  via IPP-Protokoll: mit lokaler Filterung (Default) oder ohne lokale Filterung

  Detailinformationen zu den Protokollen finden Sie in den Abschnitt 13.5.2 auf Seite 331.

Warteschlange auf LPD-Server (immer via LPD-Protokoll)
: ohne lokale Filterung (Default) oder mit lokaler Filterung

Warteschlange auf IPP-Server (immer via IPP-Protokoll)
: ohne lokale Filterung (Default) oder mit lokaler Filterung

Warteschlange auf SMB-Server (immer via SMB-Protokoll)
: mit lokaler Filterung (Default) oder ohne lokale Filterung

Warteschlange auf IPX-Server (immer via Novell IPX)
: mit lokaler Filterung (Default) oder ohne lokale Filterung

Warteschlange via sonstiger URI mit lokaler Filterung oder ohne lokale Filterung

Bei Punkt 2 sind die Voreinstellungen in der Regel ausreichend; im Zweifelsfall vgl. den oben genannten Portal-Artikel.

Bei Punkt 3 sind mit YaST die folgenden Schritte erforderlich:

'YaST Druckerkonfiguration starten' → 'Ändern...' → 'Erweitert' → 'CUPS-Servereinstellungen'

Dann: 'Adressen durchsuchen' → 'Hinzufügen' Dort ist die Broadcast-IP-Adresse des Netzwerks oder `@LOCAL` einzutragen.

Die Konfiguration wird beendet mit den folgenden Aktionen (alle Buttons befinden sich immer unten rechts): 'OK' → 'Weiter' → 'Übernehmen' → 'Beenden'

2.4.4 Festplatten-Controller

Normalerweise konfiguriert YaST den Festplatten-Contoller Ihres Systems während der Installation. Wenn Sie zusätzliche Controller einbauen, können Sie deren Einbindung in das System mit diesem YaST-Modul erledigen. Sie können hier auch die bestehende Konfiguration ändern, was aber normalerweise nicht notwendig sein sollte.

Der Dialog bietet eine Liste von erkannten Festplatten-Controllern und erlaubt eine Zuordnung des passenden Kernel-Moduls mit spezifischen Parametern. Mit 'Laden des Moduls testen' sollten Sie überprüfen, ob die aktuellen Einstellungen funktionieren, bevor sie dauerhaft im System gespeichert werden.

Achtung

Konfiguration des Festplatten-Controllers

Testen Sie die gewünschte Einstellung, bevor sie dauerhaft vom System übernommen werden soll. Fehlerhafte Einstellungen können dazu führen, dass Ihr System nicht mehr startet.

Achtung

2.4.5 Grafikkarte und Monitor (SaX2)

Hinweis

S/390, zSeries: Einrichtung der grafischen Oberfläche

IBM S/390 und zSeries verfügen über keinerlei von XFree unterstützte Ein- und Ausgabegeräte. Somit entfallen sämtliche in diesem Abschnitt geschilderten Konfigurationsarbeiten. Weitere, für IBM S/390 und zSeries relevante Informationen lesen Sie ab Abschnitt 2.5 auf Seite 98.

Hinweis

Die grafische Oberfläche, der X-Server, ermöglicht die Kommunikation zwischen Hardware und Software. Desktops wie KDE und GNOME können somit Informationen auf dem Bildschirm anzeigen, mit denen der Benutzer arbeiten kann. Desktops und ähnliche Anwendungen werden oft als *Windowmanager* bezeichnet. Unter Linux gibt es viele solcher Windowmanager, die sich in Aussehen und Funktionalität stark unterscheiden können.

Die grafische Oberfläche wird bereits während der Installation eingerichtet. Wenn Sie die Werte verbessern oder beispielsweise im laufenden System einen anderen Monitor anschließen wollen, haben Sie mit diesem YaST-Modul die Möglichkeit dazu. Vor einer eventuellen Änderung wird die aktuelle Konfiguration gespeichert. Danach gelangen Sie in denselben Dialog wie bei der Installation von SUSE LINUX. Sie haben die Wahl zwischen 'Nur Textmodus' und der grafischen Oberfläche. Für letztere werden die aktuellen Werte angezeigt: die Bildschirmauflösung, die Farbtiefe, die Bild-Wiederholfrequenz, sowie Hersteller und Typ Ihres Monitors, falls dieser automatisch erkannt wurde. Falls Sie Ihr System gerade installieren oder eine neue Grafikkarte eingebaut haben und diese zum erstenmal initialisiert wird, erscheint zusätzlich ein kleines Fenster, in dem Sie gefragt werden, ob Sie 3D-Beschleunigung für Ihre Grafikkarte aktivieren wollen.

Klicken Sie auf 'Ändern'. Jetzt startet SaX2, das Tool zum Konfigurieren der Eingabe- und Anzeigegeräte, in einem separaten Fenster (Abb. 2.9 auf der nächsten Seite).

SaX2 – Hauptfenster

In der linken Navigationsleiste sehen Sie vier Hauptpunkte: 'Anzeige', 'Eingabegeräte', 'Multihead' und 'AccessX'. Unter 'Anzeige' können Sie Ihren Monitor, Ihre Grafikkarte, Farbtiefe und Auflösung sowie Lage und Größe des dargestellten Bildes einrichten. Unter 'Eingabegeräte' konfigurieren Sie Tastatur und Maus sowie bei Bedarf einen Touchscreen-Monitor

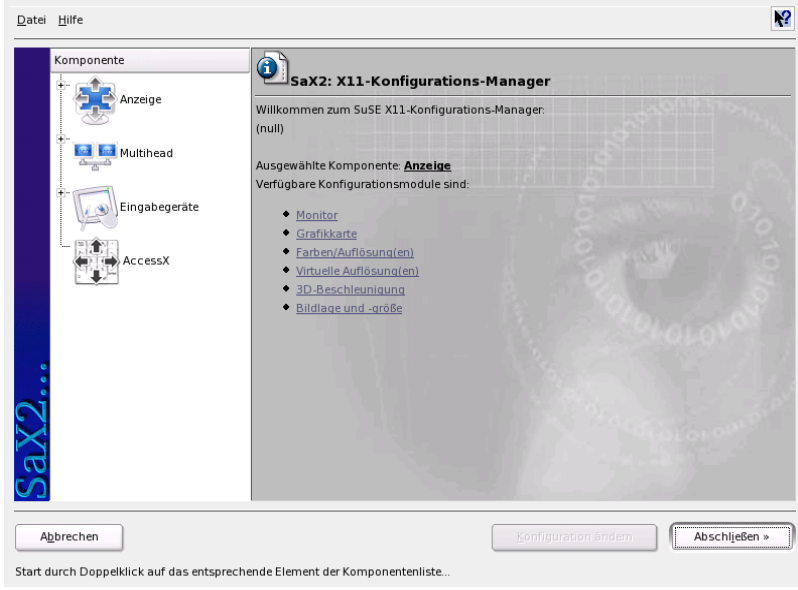

Abbildung 2.9: *Das Hauptfenster von SaX2*

und ein Grafiktablett. Im 'Multihead'-Menü richten Sie einen Mehrbildschirmbetrieb ein (s. Abschnitt 2.4.5 auf Seite 87). Sie können den Modus der Multihead-Anzeige sowie die Anordnung der Bildschirme auf Ihrem Schreibtisch festlegen. 'AccessX' ist ein hilfreiches Tool zur Steuerung des Mauszeigers mit dem Nummerntastenblock für den Fall, dass Sie einen Rechner ohne Maus booten oder die Maus noch nicht funktioniert. Hier können Sie die Geschwindigkeit des Mauszeigers, der dann mit dem Nummerntastenblock bedient wird, ändern.

Bei Monitor und Grafikkarte stellen Sie Ihre jeweiligen Modelle ein. In aller Regel werden Bildschirm und Grafikkarte automatisch vom System erkannt. Dann sind hier keine Einstellungen nötig.

Falls Ihr Monitor nicht automatisch erkannt wird, gelangen Sie automatisch in den Monitorauswahldialog. Die Hersteller- und Geräteliste bietet eine große Auswahl an Modellen, aus der Sie Ihren Monitor wählen können, oder Sie geben die Werte, die Sie der Anleitung Ihres Monitors entnehmen, manuell ein oder wählen vordefinierte Einstellungen, die so genannten Vesa-Modi.

Wenn Sie nach Abschluss Ihrer Einstellungen für Ihren Monitor und Ihre Grafikkarte hier im Hauptfenster auf 'Abschließen' klicken, haben Sie die Möglichkeit, einen Test Ihrer Einstellungen durchzuführen. Damit können Sie sicherstellen, dass Ihre Konfiguration problemlos von Ihren Geräten übernommen wurde. Falls Sie kein ruhiges Bild erhalten, brechen Sie den Test bitte sofort mit der Taste Esc ab und reduzieren Sie die Werte für die Bildwiederholfrequenz und/oder für Auflösung/Farbtiefe. Alle Ihre vorgenommenen Änderungen, ganz gleich ob Sie den Test durchgeführt haben oder nicht, werden erst aktiv, wenn Sie das grafische System, den X-Server, neu starten. Wenn Sie KDE benutzen, reicht es, wenn Sie sich einmal aus- und wieder einloggen.

Anzeige

Gehen Sie auf 'Konfiguration ändern' → 'Eigenschaften', erscheint ein Fenster mit den drei Reitern 'Monitor', 'Frequenzen' und 'Erweitert':

'Monitor' Hier wählen Sie im linken Fensterteil den Hersteller und im rechten Ihr Modell aus. Falls Sie Disketten mit Linux-Treibern für Ihren Monitor haben, können Sie diese nach Klick auf den Button 'Treiberdiskette' einspielen.

'Frequenzen' Hier können Sie die jeweiligen Horizontal- und Vertikalfrequenzen für Ihren Bildschirm eintragen. Die Vertikalfrequenz ist eine andere Bezeichnung für die Bildwiederholfrequenz. Normalerweise werden aus dem Modell die jeweiligen zulässigen Wertebereiche ausgelesen und hier eingetragen. Sie brauchen sie i.d.R. nicht zu ändern.

'Erweitert' Hier können Sie noch einige Optionen für Ihren Bildschirm eintragen. Im oberen Auswahlfeld legen Sie fest, mit welcher Methode die Bildschirmauflösung und -geometrie berechnet werden. Nehmen Sie hier nur Änderungen vor, wenn der Monitor fehlerhaft angesteuert wird, d.h. kein stabiles Bild zu erkennen ist. Weiter können Sie die Größe des dargestellten Bildes ändern und den Stromsparmodus DPMS aktivieren.

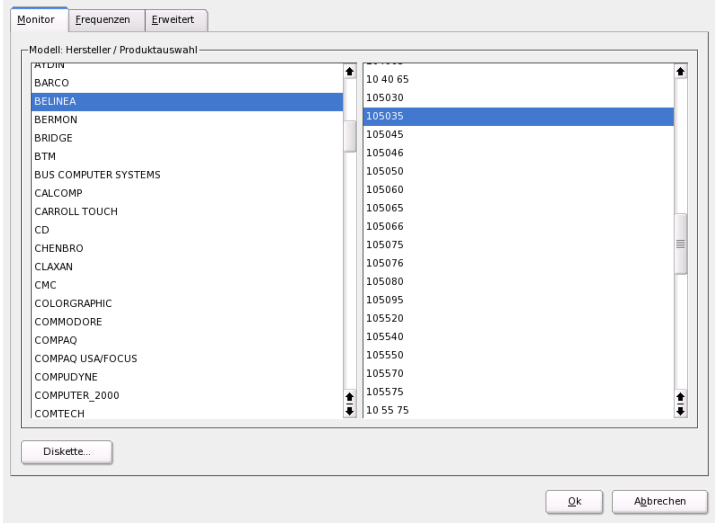

Abbildung 2.10: *SaX2: Die Auswahl des Monitors*

Achtung

Konfiguration der Monitorfrequenzen

Lassen Sie trotz der eingebauten Schutzmechanismen insbesondere bei der manuellen Eingabe der zulässigen Frequenzen besondere Sorgfalt walten. Falsche Werte können zur Zerstörung des Monitors führen. Schlagen Sie die Werte gegebenenfalls im Handbuch Ihres Monitors nach.

Achtung

Grafikkarte

Im Grafikkartendialog gibt es zwei Reiter: ‘Allgemein’ und ‘Erweitert’:

‘Allgemein’ – Hier stellen Sie wie oben bei der Monitoreinrichtung links den Hersteller und rechts das Modell Ihrer Grafikkarte ein.

‘Erweitert’ – Sie können hier rechts einstellen, ob Sie Ihren Bildschirm nach links oder in die Senkrechte gedreht haben (v. a. bei manchen drehbaren TFT-Bildschirmen sinnvoll). Die Eintragungen für die BusID sind nur beim

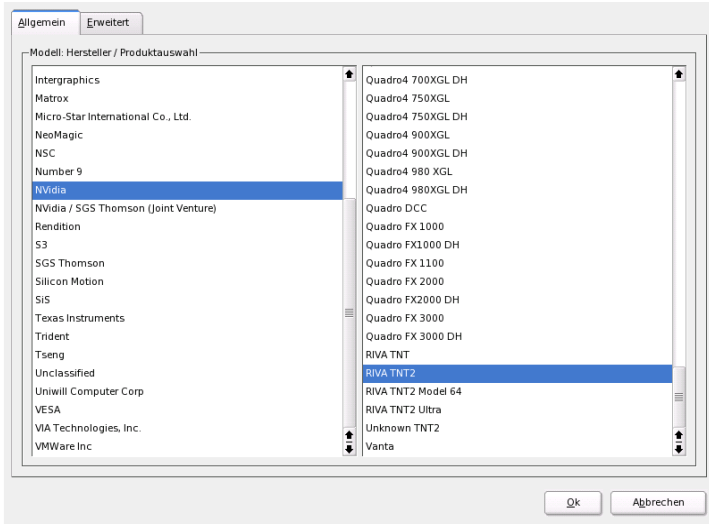

Abbildung 2.11: *SaX2: Die Auswahl der Grafikkarte*

Betrieb mehrerer Bildschirme von Bedeutung. Hier brauchen Sie normalerweise nichts zu ändern. Auch die Kartenoptionen sollten Sie nicht ändern, wenn Sie die Bedeutung der Optionen nicht kennen. Lesen Sie hierzu bei Bedarf in der Dokumentation Ihrer Grafikkarte nach.

Farben/Auflösung(en)

Auch hier gibt es wieder drei Reiter: 'Farben', 'Auflösung' und 'Erweitert'.

'Farben' Bei der Auswahl der Farbtiefe stehen Ihnen abhängig von der verwendeten Hardware die Einstellungen 16, 256, 32768, 65536 und 16,7 Millionen Farben bei 4, 8, 15, 16 oder 24 Bit zur Verfügung. Für eine brauchbare Darstellung sollten Sie wenigstens 256 Farben einstellen.

'Auflösung' Beim Erkennen der Hardware wird diese abgefragt und Kombinationen aus Auflösung und Farbtiefen angeboten, die von Ihrer Hardware fehlerfrei angezeigt werden können. Daher ist die Gefahr, dass Sie durch falsche Einstellungen Ihre Hardware beschädigen, unter SUSE LINUX sehr gering. Wenn Sie allerdings die Auflösung manuell ändern, sollten Sie sich unbedingt in der Dokumen-

tation zu Ihrer Hardware informieren, ob diese Ihre neu eingestellten Werte problemlos darstellen kann.

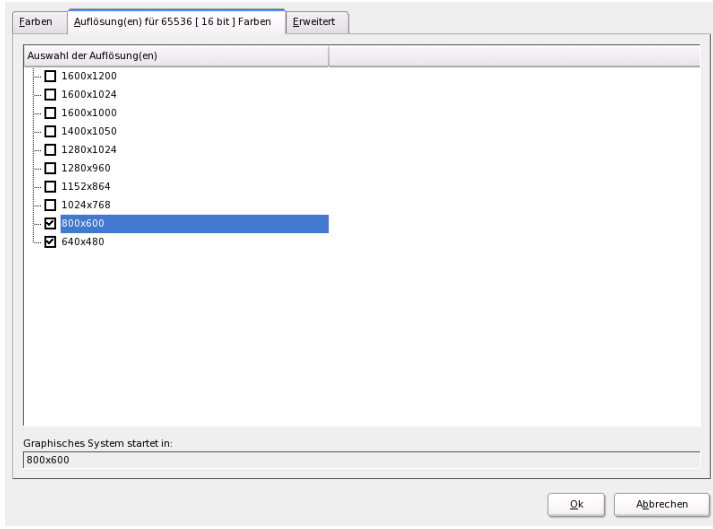

Abbildung 2.12: *SaX2: Auflösungen einstellen*

'Erweitert' Hier können Sie zu den Auflösungen, die im vorigen Reiter angeboten wurden, eigene hinzufügen, die dann in die Auswahl mitaufgenommen werden.

Virtuelle Auflösung

Jede Oberfläche besitzt ihre eigene Auflösung, die über den ganzen Bildschirm sichtbar ist. Neben dieser Auflösung kann eine weitere Auflösung eingestellt werden, die größer als der sichtbare Bereich des Bildschirms ist. Wenn Sie die Kanten des Bildschirms mit der Maus verlassen, wird der virtuelle Bereich in den sichtbaren Bereich des Monitors geschoben. An der Pixelgröße ändert sich dabei nichts, jedoch ist die Nutzfläche der Oberfläche größer. Dies bezeichnet man als virtuelle Auflösung.

Das Einstellen der virtuellen Auflösung kann auf zwei verschiedene Arten geschehen:

'Über Drag&Drop' – Befindet sich die Maus auf dem angezeigten Monitorbild, so verändert sich der Mauszeiger zu einem Fadenkreuz. Halten Sie

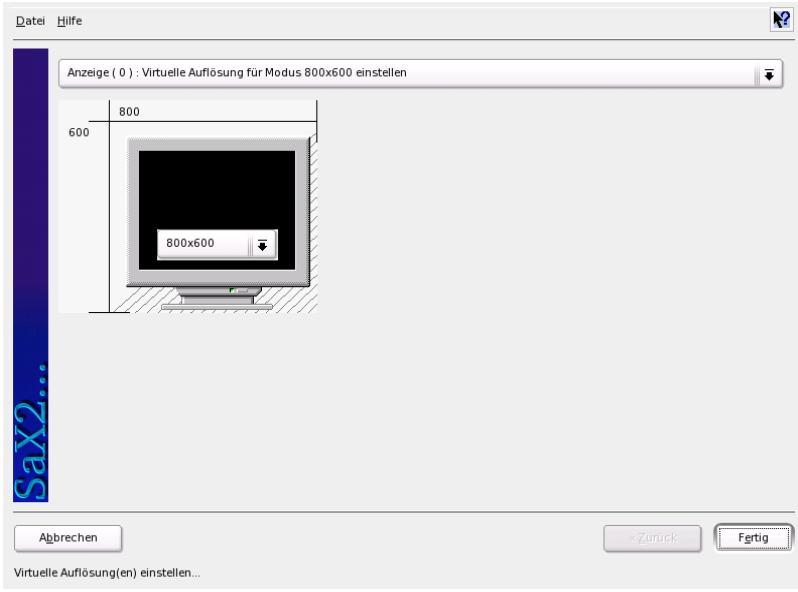

Abbildung 2.13: *SaX2: Virtuelle Auflösung einstellen*

die linke Maustaste gedrückt und bewegen Sie gleichzeitig die Maus, so verändert sich die Größe der Rasterfläche. Die Größe der Rasterfläche zeigt den Bereich der virtuellen Auflösung entsprechend der realen, durch das Monitorbild dargestellten Auflösung an. Diese Einstellmethode empfiehlt sich immer dann, wenn Sie nur einen bestimmten Bereich, über dessen Größe Sie sich noch nicht ganz sicher sind, als virtuellen Bereich einstellen wollen.

'Durch Auswahl aus dem Popup-Menü' – Über das Popup-Menü, das sich immer in der Mitte der Rasterfläche befindet, sehen Sie die aktuell eingestellte virtuelle Auflösung. Wenn Sie bereits wissen, dass Sie eine Standardauflösung als virtuelle Auflösung definieren wollen, wählen Sie einfach über das Menü eine entsprechende Auflösung aus.

Bildlage und -größe

Hier können Sie mit Hilfe der Pfeile die Größe und Position des angezeigten Bildes genau justieren (vgl. Abb. 2.14 auf der nächsten Seite). Wenn Sie mit einer Multihead-Umgebung arbeiten (mehr als ein Bildschirm), kön-

nen Sie mit dem Button 'Nächster Bildschirm' zu Ihren weiteren Monitoren springen, um dort ebenfalls Größe und Position festzulegen. Mit 'Speichern' sichern Sie Ihre Einstellungen.

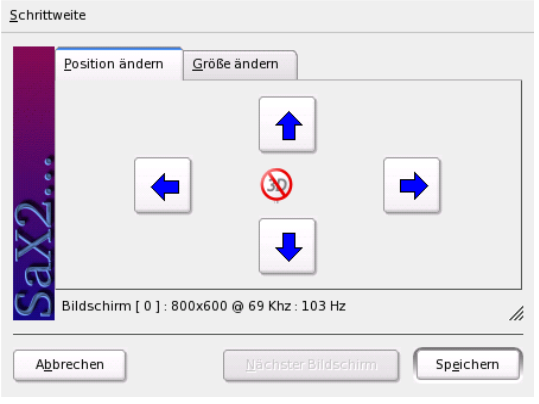

Abbildung 2.14: *SaX2: Anpassung der Bildgeometrie*

Multihead

Wenn Sie mehr als eine Grafikkarte in Ihren Rechner eingebaut haben oder eine Grafikkarte mit mehreren Ausgängen besitzen, können Sie mehrere Bildschirme an Ihrem System betreiben. Betreiben Sie zwei Bildschirme, wird das *Dualhead*, bei mehr als zwei *Multihead* genannt. SaX2 erkennt automatisch, wenn sich im System mehrere Grafikkarten befinden, und bereitet die Konfiguration entsprechend darauf vor. In dem Multihead-Dialog von SaX können Sie den Multihead-Modus und die Anordnung Ihrer Bildschirme festlegen. Drei Modi stehen zur Verfügung: 'Traditionell' (default), 'Xinerama' und 'Cloned':

'Traditionelles Multihead' Sie haben mit jedem Monitor eine eigenständige Einheit. Lediglich der Mauszeiger kann zwischen den Bildschirmen wechseln.

'Cloned Multihead' Dieser Modus ist überwiegend für Präsentationen und Messen von Bedeutung und vor allem bei großen Bildschirmwänden sehr effektvoll. Jeder Monitor hat in diesem Modus den gleichen Inhalt. Die Maus ist in diesem Modus nur auf dem Hauptschirm zu sehen.

'Xinerama Multihead' Alle Bildschirme verschmelzen zu einem einzigen großen, das heisst Programmfenster können frei auf allen Monitoren platziert werden oder auf eine Größe, die mehr als einen Monitor umfasst, aufgezogen werden.

Unter dem Layout einer Multihead-Umgebung versteht man die Anordnung und Nachbarschaftsbeziehungen der einzelnen Bildschirme. SaX2 legt standardmäßig in der Reihenfolge der erkannten Grafikkarten ein Standardlayout an, das alle Bildschirme in einer Linie von links nach rechts anordnet. Im 'Layout'-Dialog des Multihead-Tools legen Sie fest, wie die Monitore auf Ihrem Schreibtisch angeordnet sind, indem Sie einfach mit der Maus die Bildschirmsymbole auf der Gitterwand verschieben.

Nachdem Sie den Layout-Dialog abgeschlossen haben, können Sie die neue Konfiguration durch Klick auf den Button 'Test' überprüfen.

Bitte beachten Sie, dass Linux derzeit keine 3D-Unterstützung in einer Xinerama-Multiheadumgebung bietet. SaX2 schaltet die 3D Unterstützung in diesem Fall ab.

Eingabegeräte

Maus Wenn die Maus bereits funktioniert, müssen Sie hier nichts weiter tun. Sollte die Maus jedoch nicht funktionieren, können Sie sie über den Ziffernblock der Tastatur wie im Abschnitt 2.4.5 auf der nächsten Seite beschrieben steuern.

Falls die automatische Erkennung fehlschlägt, müssen Sie Ihre Maus manuell konfigurieren. Der Dokumentation zu Ihrer Maus können Sie eine Beschreibung des Typs entnehmen. Wählen Sie diesen aus der Liste der unterstützten Maustypen aus. Wenn der richtige Maustyp markiert ist, bestätigen Sie das durch Klick mit der Taste (5) auf dem Ziffernblock.

Tastatur In diesem Dialog legen Sie in dem oberen Auswahlfeld fest, welche Tastatur Sie benutzen. Darunter wählen Sie die Sprache für Ihr Tastaturlayout, d.h. für die länderspezifische Lage der Tasten. In dem Testfeld schließlich können Sie durch Eingabe von Sonderzeichen, zum Beispiel ö, ä, ü oder ß, feststellen, ob Ihr gewähltes Sprachlayout korrekt übernommen wurde.

Die Checkbox, mit der Sie die Eingabe von akzentuierten Buchstaben ein- und ausschalten können, sollten Sie im Normalfall so belassen, wie sie für die jeweilige Sprache voreingestellt ist. Mit 'Beenden' übernehmen Sie die neuen Einstellungen in Ihr System.

Touchscreen Derzeit werden von XFree86 Touchscreens der Marken Microtouch und Elo TouchSystems unterstützt. SaX2 kann in diesem Fall nur den Monitor automatisch erkennen, nicht aber den Toucher. Der Toucher ist wiederum wie ein Eingabegerät anzusehen. Folgende Schritte sind zur Einrichtung nötig:

1. Starten Sie SaX2 und wechseln Sie zu 'Eingabegeräte' -> 'Touchscreens'.
2. Klicken Sie auf 'Hinzufügen' und fügen Sie einen Touchscreen hinzu.
3. Speichern Sie die Konfiguration mit 'Beenden' ab. Ein Test der Konfiguration ist nicht zwingend erforderlich.

Touchscreens besitzen eine Vielzahl von Optionen und müssen in den meisten Fällen zuerst kalibriert werden. Unter Linux gibt es dazu leider kein allgemeines Werkzeug. Zu den Größenverhältnissen der Touchscreens sind in die Standardkonfigurationen sinnvolle Default-Werte integriert, so dass hier i. d. R. keine zusätzliche Konfiguration nötig wird.

Grafiktablet Derzeit werden von XFree86 noch einige Grafiktablets unterstützt. SaX2 bietet dazu die Konfiguration über USB bzw. serielle Schnittstelle an. Ein Grafiktablet ist aus der Sicht der Konfiguration wie eine Maus anzusehen oder, allgemeiner ausgedrückt, wie ein Eingabegerät. Es empfiehlt sich folgende Vorgehensweise:

1. Starten Sie SaX2 und wechseln Sie zu 'Eingabegeräte' -> 'Grafiktablet'.
2. Klicken Sie auf 'Hinzufügen', wählen Sie im folgenden Dialog den Hersteller und und fügen Sie ein Grafiktablet aus der angebotenen Liste hinzu.
3. Kreuzen Sie dann rechts in den Checkboxen an, ob Sie noch einen Stift und/oder einen Radierer angeschlossen haben.
4. Prüfen Sie bei einem seriellen Tablet wie bei allen hinzugefügten Geräten, ob der Anschluss richtig ist: `/dev/ttyS0` bezeichnet die erste serielle Schnittstelle, `/dev/ttyS1` die zweite und so weiter.
5. Speichern Sie die Konfiguration durch Klick auf 'Beenden' ab.

AccessX

Wenn Sie Ihren Rechner ohne Maus betreiben und nach dem Start von SaX2 AccessX aktivieren, können Sie den Mauszeiger auf Ihrem Bildschirm mit dem Nummerntastenblock Ihrer Tastatur steuern (siehe Tabelle 2.1 auf der nächsten Seite).

Tabelle 2.1: *AccessX – Bedienung der Maus über den Nummernblock*

Taste	Beschreibung
(÷)	Aktiviert die linke Maustaste
(×)	Aktiviert die mittlere Maustaste
(−)	Aktiviert die rechte Maustaste
(5)	Diese Taste löst einen Klick des zuvor aktivierten Mausbuttons aus. Wurde kein Mausbutton aktiviert, wird die linke Maustaste benutzt. Die Aktivierung der jeweiligen Taste wird nach dem Klick wieder auf die Standardeinstellung gesetzt.
(+)	Diese Taste wirkt wie die Taste (5), mit dem Unterschied, dass dadurch ein Doppelklick ausgelöst wird.
(0)	Diese Taste wirkt wie die Taste (5), mit dem Unterschied, dass sie nur einen Druck des Mausbuttons bewirkt und diesen beibehält.
(Entf)	Diese Taste löst den Druck auf einen Mausbutton, der mit der Taste (0) erzeugt wurde.
(7)	Bewegt die Maus nach links oben
(8)	Bewegt die Maus geradlinig nach oben
(9)	Bewegt die Maus nach rechts oben
(4)	Bewegt die Maus nach links
(6)	Bewegt die Maus nach rechts
(1)	Bewegt die Maus nach links unten
(2)	Bewegt die Maus geradlinig nach unten
(3)	Bewegt die Maus nach rechts unten

Sie können nun mit dem Schieberegler einstellen, wie schnell sich Ihr

Mauszeiger bei Druck der jeweiligen Tasten bewegen soll.

Weiterführende Informationen

Weiterführende Informationen über das X-Window-System, seine Geschichte und seine Eigenschaften finden Sie im Kapitel 12 auf Seite 305.

2.4.6 Hardware-Informationen

YaST führt für die Konfiguration von Hardwarekomponenten eine Hardware-Erkennung durch. Die erkannten technischen Daten werden in diesem Dialog angezeigt. Dies ist insbesondere dann nützlich, wenn Sie z. B. eine Support-Anfrage stellen wollen – dafür brauchen Sie Informationen zu Ihrer Hardware.

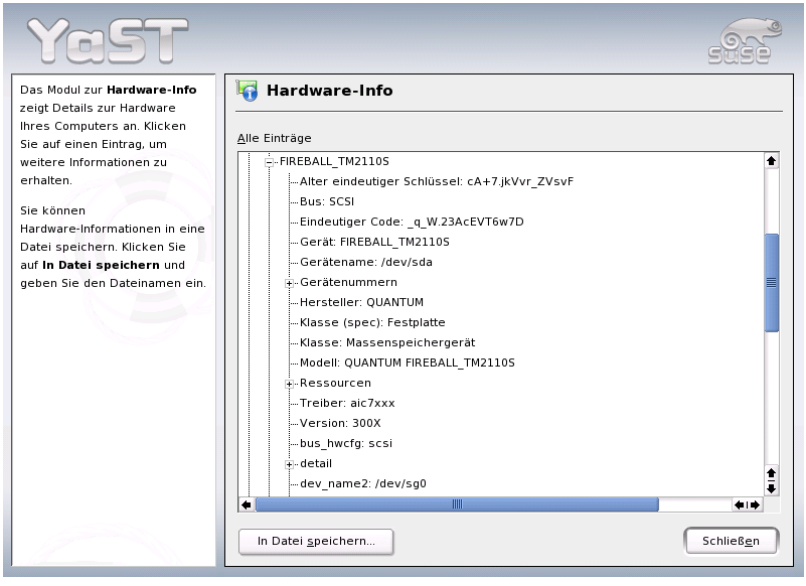

Abbildung 2.15: *Hardwareinformationen anzeigen*

2.4.7 IDE DMA-Modus

Dieses Modul ermöglicht Ihnen, bei installiertem System den sog. DMA-Modus für Ihre (IDE-) Festplatte(n) und Ihre (IDE-) CD/DVD-Laufwerke

zu aktivieren oder zu deaktivieren. Bei SCSI-Geräten ist dieses Modul funktionslos. DMA-Modi können die Leistungsfähigkeit bzw. die Geschwindigkeit der Datenübertragung in Ihrem System erheblich steigern.

Der aktuelle Kernel von SUSE LINUX aktiviert bei der Systeminstallation DMA automatisch für Festplatten und lässt ihn für CD-Laufwerke deaktiviert, da in der Vergangenheit bei standardmäßiger DMA-Aktivierung für alle Laufwerke des öfteren Probleme bei CD-Laufwerken aufgetreten sind. Sie können nachträglich mit dem DMA-Modul für Ihre Laufwerke entscheiden, ob Sie DMA aktivieren oder nicht. Sollten z.B. bei Ihrem Festplattenbetrieb Probleme auftauchen, kann es hilfreich sein, DMA zu deaktivieren. Umgekehrt steigern Sie die Datenübertragungsrate Ihres CD-Laufwerks, wenn Sie DMA dafür aktivieren und das Laufwerk den Modus ohne Probleme unterstützt.

Hinweis

DMA (=**D**irect **M**emory **A**ccess) bedeutet Direkter Speicherzugriff, d. h. Laufwerke können Ihre Daten direkt in den Arbeitsspeicher übertragen ohne den Umweg über die Prozessorsteuerung.

Hinweis

2.4.8 Maus

Mit diesem YaST-Modul stellen Sie das aktuell verwendete Maus-Modell ein. Weil die Vorgehensweise für die Auswahl der Maus schon im Rahmen der benutzerdefinierten Installation erklärt wurde, verweisen wir hier auf den Abschnitt 1.7.3 auf Seite 18.

2.4.9 Scanner

Wenn Sie Ihren Scanner angeschlossen und eingeschaltet haben, sollte beim Start dieses YaST-Moduls Ihr Scanner automatisch erkannt werden. In diesem Fall erscheint der Dialog zur Installation des Scanners. Falls kein Scanner erkannt wird, geht es weiter mit der manuellen Konfiguration. Wenn Sie bereits einen oder mehrere Scanner installiert haben sollten, erscheint zunächst eine Übersichtstabelle mit einer Liste vorhandener Scanner, die bearbeitet oder gelöscht werden können. Mit ‘Hinzufügen’ richten Sie ein neues Gerät ein.

Als Nächstes wird eine Installation mit Standardeinstellungen durchgeführt. Wenn die Installation erfolgreich war, erscheint eine entsprechende Meldung. Nun können Sie Ihren Scanner testen, indem Sie eine Vorlage darauf legen und dann auf 'Test' klicken.

Scanner wurde nicht erkannt

Beachten Sie, dass nur unterstützte Scanner automatisch erkannt werden können. Scanner, die an einer anderen Maschine im Netzwerk betrieben werden, werden auch nicht erkannt. Unterscheiden Sie zur manuellen Konfiguration zwischen einem USB-, SCSI- oder Netzwerkscanner.

USB-Scanner Hier muss der Hersteller bzw. das Modell eingegeben werden. YaST versucht, USB-Module nachzuladen. Falls Ihr Scanner sehr neu ist, kann es sein, dass die Module nicht automatisch geladen werden können. In diesem Fall gelangen Sie weiter in einen Dialog, in dem Sie die Möglichkeit haben, das USB-Modul per Hand nachzuladen. Lesen Sie hierzu den YaST-Hilfetext.

SCSI-Scanner Geben Sie das Device an (zum Beispiel `/dev/sg0`). Hinweis: Ein SCSI-Scanner darf nicht im laufenden System angeschlossen oder ausgesteckt werden. Fahren Sie zuerst das System herunter.

Netzwerk-Scanner Hier benötigen Sie die IP-Adresse bzw. den Hostnamen. Lesen Sie zur Konfiguration eines Netzwerk-Scanners den Supportdatenbank-Artikel *Scanner unter Linux* (`http://sdb.suse.de/`, Stichwortsuche `Scanner`).

Wenn Ihr Scanner nicht erkannt wurde, ist das Gerät wahrscheinlich nicht unterstützt. Manchmal werden jedoch auch unterstützte Scanner nicht erkannt. Hier hilft Ihnen gegebenenfalls die manuelle Scanner-Auswahl weiter. Wenn Sie in der Hersteller- und Modellliste Ihren Scanner identifizieren können, wählen Sie ihn einfach an; falls nicht, gehen Sie lieber auf 'Abbrechen'. Informationen zu Scannern, die mit Linux funktionieren, finden Sie unter `http://cdb.suse.de`, `http://sdb.suse.de` oder `http://www.mostang.com/sane` .

Achtung

Manuelle Zuordnung des Scanners

Die manuelle Zuordnung des Scanners sollten Sie nur dann vornehmen, wenn Sie sich sicher sind. Bei einer falschen Auswahl kann sonst Ihre Hardware Schaden nehmen.

Achtung

Fehlerbehebung

Wenn Ihr Scanner nicht erkannt wurde, sind folgende Ursachen möglich:

- Der Scanner wird nicht unterstützt. Unter `http://www.suse.de/sdb` finden Sie eine Liste mit Geräten, die zu Linux kompatibel sind.
- Ihr SCSI-Controller ist nicht korrekt installiert.
- Es gibt Terminierungs-Probleme mit Ihrer SCSI-Schnittstelle.
- Ihr SCSI-Kabel überschreitet die zulässige Länge.
- Ihr Scanner hat einen SCSI-Light-Controller, der von Linux nicht unterstützt wird.
- Ihr Scanner könnte defekt sein.

Achtung

Bei einem SCSI-Scanner darf das Gerät auf keinen Fall im laufenden System angeschlossen oder ausgesteckt werden. Fahren Sie bitte zuerst Ihren Rechner herunter.

Achtung

2.4.10 Sound

YaST versucht beim Aufruf des Sound-Konfigurationstools, Ihre Soundkarte automatisch zu erkennen. Sie können eine oder mehrere Soundkarten einrichten. Falls man mehrere Soundkarten verwenden möchte, wählt man zuerst eine der zu konfigurierenden Karten aus. Mit dem Button 'Konfigurieren' gelangen Sie weiter zum Menü 'Setup'. Über den Button 'Bearbeiten' kann man bereits konfigurierte Soundkarten unter 'Soundkonfiguration' editieren. 'Beenden' speichert die momentanen Einstellungen und schließt die Soundkonfiguration ab. Sollte YaST Ihre Soundkarte nicht automatisch erkennen, kann man über das Menü 'Soundkonfiguration' mit dem Button 'Soundkarte hinzufügen' zur 'Manuellen Auswahl der Soundkarten' gelangen. In diesem Dialog ist es möglich, eine Soundkarte und das zugehörige Modul selbst auszuwählen.

Setup

Unter 'Schnelles automatisches Setup' werden keine weiteren Konfigurationsschritte abgefragt und kein Testsound gestartet. Die Soundkarte wird fertig eingerichtet. Mit 'Normales Setup' hat man die Möglichkeit, im folgenden Menü 'Lautstärke der Soundkarte' die Ausgangslautstärke zu regeln und einen Testsound abzuspielen.

Bei 'Erweitertes Setup' mit der Möglichkeit, Optionen zu ändern, gelangt man in das Menü 'Erweiterte Optionen für die Soundkarte'. Hier kann man die Optionen der Soundmodule manuell anpassen.

Zusätzlich können Sie von hier aus Ihren Joystick einrichten, indem Sie auf die gleichnamige Checkbox klicken. Es erscheint dann ein Dialog, in dem Sie den Typ Ihres Joysticks auswählen und dann auf 'Weiter' klicken. Der gleiche Dialog erscheint auch, wenn Sie im YaST-Kontrollzentrum auf 'Joystick' klicken.

Lautstärke der Soundkarte

Unter dieser Testmaske können Sie Ihre Soundkonfiguration testen. Mit den Buttons '+' und '-' stellen Sie die Lautstärke ein. Beginnen Sie bitte bei etwa 10%, um weder Ihre Lautsprecher noch Ihr Gehör zu schädigen. Durch einen Klick auf den Button 'Test' sollte jetzt ein Testsound zu hören sein, falls nicht, regeln Sie die Lautstärke nach. Mit 'Weiter' schließen Sie die Soundkonfiguration ab und die Lautstärke wird gespeichert.

Soundkonfiguration

Mit der Option 'Löschen' kann man eine Soundkarte entfernen. Vorhandene Einträge von bereits konfigurierten Soundkarten werden in der Datei `/etc/modprobe.d/sound` deaktiviert. Unter 'Optionen' gelangt man in das Menü 'Erweiterte Optionen für die Soundkarte'. Hier kann man die Optionen der Soundmodule manuell anpassen. Im Menü 'Mixer' ist es möglich, die Pegeleinstellungen für Ein- und Ausgänge der jeweiligen Soundkarten zu konfigurieren. Mit 'Weiter' werden die neuen Werte gespeichert und mit 'Zurück' wieder auf die Standardeinstellungen zurückgesetzt. Bei 'Soundkarte hinzufügen...' können Sie weitere Soundkarten integrieren. Findet YaST automatisch eine weitere Soundkarte, gelangen Sie in das Menü 'Konfigurieren Sie eine Soundkarte'. Findet YaST keine Soundkarte, geht es direkt zu 'Manuelle Auswahl der Soundkarte'.

Wenn Sie eine Creative Soundblaster Live oder AWE verwenden, können Sie über die Option 'Soundfonts installieren' automatisch von der original

Soundblaster Treiber CD-ROM SF2-Soundfonts auf Ihre Festplatte kopieren. Diese werden im Verzeichnis `/usr/share/sfbank/creative/` abgelegt.

Über die Checkbox 'ALSA starten' kann man das Starten von ALSA beim Booten des Rechners (de-)aktivieren. Zur Wiedergabe von Midi-Dateien sollten Sie die Checkbox 'Sequenzer starten' aktiviert haben. Somit werden beim Laden der ALSA-Module die benötigten Soundmodule für die Sequenzerunterstützung mitgeladen.

Beim Aufruf von 'Beenden' wird die Lautstärke und die Konfiguration aller bis dahin installierten Soundkarten gespeichert. Die Mixereinstellungen werden in der Datei `/etc/asound.conf` abgelegt und die ALSA-Konfigurationsdaten werden am Ende der Datei `/etc/modprobe.conf` eingetragen.

Konfigurieren Sie eine Soundkarte

Wurden mehrere Soundkarten gefunden, wählen Sie unter 'Liste der automatisch erkannten...' Ihre gewünschte Karte aus. Mit 'Weiter' gelangen Sie nun zum Menüpunkt 'Setup'. Wird die Soundkarte nicht automatisch gefunden, wählen Sie den Punkt 'von der Liste wählen' an und mit 'Weiter' gelangt man in das Menü 'Manuelle Auswahl der Soundkarte'.

Manuelle Auswahl der Soundkarte

Falls Ihre Soundkarte nicht automatisch erkannt wurde, wird eine Liste von Soundkartentreibern und Soundkartenmodellen angezeigt, aus der Sie eine Auswahl treffen können. Mit der Auswahl 'Alle' können Sie die komplette Liste der unterstützten Soundkarten ansehen.

Sehen Sie gegebenenfalls in der Dokumentation zu Ihrer Soundkarte nach, um die nötigen Informationen zu erhalten. Des Weiteren finden Sie auch eine Aufstellung der von ALSA unterstützten Soundkarten mit den jeweils zugehörigen Soundmodulen unter `/usr/share/doc/packages/alsa/cards.txt` und `http://www.alsa-project.org/~goemon/`. Nach der Auswahl gelangt man über 'Weiter' wieder in das Menü 'Setup'.

2.4.11 S/390, zSeries: ZFCP

Um dem installierten System zusätzliche ZFCP-Geräte hinzuzufügen, verwenden Sie das YaST ZFCP-Modul ('Hardware' → 'ZFCP'). Wählen Sie zunächst 'Hinzufügen' aus. Im nächsten Dialog wählen Sie die 'Kanalnummer' aus einer Drop-Down Liste und legen 'WWPN' und 'FCP-LUN' fest.

Schließen Sie die Konfiguration ab, indem Sie den Dialog mit ‘Weiter’ und ‘Schließen’ verlassen. Um sicherzugehen, dass das neue Gerät tatsächlich in die Konfiguration integriert wurde, überprüfen Sie die Ausgabe von `cat /proc/scsi/scsi`.

2.5 Netzwerkgeräte

Die YaST-Konfigurationsbeschreibung für alle Typen von unterstützen Netzwerkgeräten sowie Hintergrundinformationen zur Einbindung ins Netzwerk lesen Sie in Abschnitt 21.4 auf Seite 481 nach.

2.6 Netzwerk-Dienste

2.6.1 DHCP-Server

Mit YaST können Sie in wenigen Arbeitsschritten einen eigenen DHCP-Server aufsetzen. In Kapitel 21.11 auf Seite 563 lesen Sie Grundlagen zum Thema und die einzelnen YaST Konfigurationsschritte nach.

2.6.2 Hostname und DNS

Dieses Modul dient zur separaten Konfiguration von Hostname und DNS, wenn diese Angaben nicht bereits bei der Konfiguration des Netzwerkgeräts gemacht wurden.

2.6.3 NFS-Client und NFS-Server

NFS gibt Ihnen die Möglichkeit, unter Linux einen so genannten Fileserver zu betreiben, auf den die Mitglieder Ihres Netzwerkes zugreifen können. Auf diesem Fileserver stellen Sie z. B. bestimmte Programme und Dateien oder auch Speicherplatz für die Benutzer zur Verfügung. In dem Modul ‘NFS-Server’ legen Sie dann fest, dass Ihr Rechner als NFS-Server fungieren soll und welche Verzeichnisse exportiert, d.h. von den Benutzern des Netzwerks benutzt werden können. Jeder Benutzer (der die Rechte dazu erteilt bekommt), kann dann diese Verzeichnisse in seinen eigenen Dateibaum hineinmounten. Die YaST-Modulbeschreibung und Hintergründe zu NFS lesen Sie in Abschnitt 21.10 auf Seite 557 nach.

2.6.4 Konfiguration eines Samba-Servers

Richten Sie einen Samba-Server ein, um Ressourcen wie Dateien oder Drucker mit Windows-Rechnern zu teilen. Definieren Sie in der erste Maske, welche Rolle der Samba-Server übernehmen soll. Sie können Ihn deaktivieren, als Datei- und Druckserver verwenden, als Backup Domain Controller oder Primary Domain Controller einsetzen. Ein Datei- und Druckserver stellt nur Verzeichnisse und Drucker zur Verfügung. Ein Domain Controller erlaubt seinen Clients sich auf einer Windows-Domain einzuloggen. Der Primary Domain Controller verwaltet selbst Benutzer und Passwörter, ein Backup Domain Controller dagagen verwendet einen anderen Domain Controller zur Authentifizierung der Benutzer. Weiterführende Informationen zu Samba finden Sie im Abschnitt 24.1 auf Seite 634.

2.6.5 Konfiguration eines Samba-Clients

Konfigurieren Sie einen Samba-Client, um einfach auf Ressourcen (Dateien oder Drucker) auf dem Samba-Server zuzugreifen. Tragen Sie im Dialog Samba Workgroup die Domain oder Arbeitsgruppe ein. Über die Schaltfläche 'Auswählen' werden alle verfügbaren Gruppen und Domains angezeigt. Sie können dann mit Mausklick auswählen. Aktivieren Sie die Checkbox 'SMB-Informationen auch für die Linux-Authentifizierung verwenden' wird die Benutzerauthentifizierung über den Samba-Server laufen. Haben Sie alle Einstellungen vorgenommen, klicken Sie auf 'Beenden', um die Konfiguration abzuschließen.

2.6.6 NTP Client

NTP (engl. *Network Time Protocol*) ist ein Protokoll, um die Uhrzeit von Rechnern über ein Netzwerk zu synchronisieren. Mit dem entsprechenden YaST-Modul können Sie durch 'Hinzufügen' einen Typ auswählen. Es stehen eine Reihe von Auswahlmöglichkeiten zur Verfügung, von denen 'Server' und 'Funkuhr' am Häufigsten verwendet werden dürften. Bei 'Funkuhr' wird allerdings zusätzlich eine entsprechende Hardware benötigt.

Wird 'Server' angewählt, müssen Sie die Adresse eines NTP-Servers eingeben. Sie können auch einen öffentlichen NTP-Server angeben, den Sie unter `http://www.eecis.udel.edu/~mills/ntp/servers.html` finden können. Bestätigen Sie mit 'OK'.

Um den NTP-Daemon beim Systemstart zu starten, wählen Sie 'When booting system' an. Ihre Einstellungen sichern Sie mit 'Beenden'.

Weitere Informationen zum Thema NTP erhalten Sie im Abschnitt 21.12 auf Seite 577.

2.6.7 Routing

Nähere Informationen zum Thema Routing finden Sie in Abschnitt 21.5 auf Seite 497.

2.6.8 Mail Transfer Agent

Mit diesem Konfigurationsmodul können Sie Ihre Mail-Einstellungen anpassen, wenn Sie Ihre E-Mails mit sendmail, postfix oder mittels des SMTP-Servers Ihres Providers versenden. Mail herunterladen können Sie mit dem Programm fetchmail, zu dem Sie hier ebenfalls die Daten des POP3- oder IMAP-Servers Ihres Providers eintragen können.

Alternativ können Sie in einem Mail-Programm Ihrer Wahl, z.B. KMail , einfach Ihre POP- und SMTP-Zugangsdaten einstellen, wie Sie es bisher gewohnt waren (Empfang mit POP3, Versand mit SMTP). Sie benötigen dann dieses Modul nicht.

Verbindungsart

Falls Sie Ihre Mail-Einstellungen über YaST vornehmen wollen, verlangt das System im ersten Dialog des E-Mail-Dialogs die Angabe der gewünschten Verbindungsart ins Internet. Sie haben folgende Alternativen:

'Permanent' Wünschen Sie eine Standleitung ins Internet, wählen Sie diese Option. Ihr Rechner wird ununterbrochen online sein, so dass keine separate Einwahl nötig ist. Befindet sich Ihr System innerhalb eines lokalen Netzwerks mit zentralem Mail-Server zum E-Mail-Versand, wählen Sie ebenfalls diese Option, um permanenten Zugang zu Ihren E-Mails zu gewährleisten.

'Einwahl' Dieser Menüpunkt betrifft alle Benutzer, die zuhause einen Rechner haben, der keinem Netzwerk angehört und sich gelegentlich ins Internet einwählen.

Keine Verbindung Wenn Sie keinen Internetzugang haben und auch keinem Netz angehören, können Sie keine E-Mails verschicken oder empfangen.

Zusätzlich können Sie per Checkbox die Virusüberprüfung Ihrer eingehend en und ausgehenden E-Mails durch AMaViS aktivieren. Das entsprechende Paket wird automatisch installiert, sobald Sie die Mail-Filterung aktivieren. In den weiteren Dialogen legen Sie den ausgehenden Mail-Server (i.A. der SMTP-Server Ihres Providers) und die Parameter für eingehende Mail fest. Verwenden Sie eine Einwahlverbindung (dial-up), können Sie verschiedene POP- bzw. IMAP-Server zum Mail-Empfang durch unterschiedliche Benutzer angeben. Schließlich können Sie über diesen Dialog optional zusätzlich Aliasnamen vergeben, Masquerading einstellen oder virtuelle Domains anlegen. Mit 'Beenden' verlassen Sie die Mail-Konfiguration.

2.6.9 Mailserver

Hinweis

LDAP-gestützte Konfiguration des Mailservers

Das Mailserver Modul des SUSE LINUX Enterprise Server funktioniert ausschließlich dann, wenn Benutzer- und Gruppenmanagement sowie DNS- und DHCP-Dienste über LDAP abgewickelt werden.

Hinweis

Das YaST Mailserver Modul ermöglicht Ihnen die Konfiguration des SUSE LINUX Enterprise Server als Mailserver. Folgende Konfigurationsschritte werden bei der Konfiguration mit YaST abgedeckt:

Globale Konfiguration Konfigurieren Sie die Identifikation Ihress Mailservers sowie maximale Größe der zu versendenden bzw. empfangenden Mail und die Art der Mailtransports.

Lokale Zustellung Konfigurieren Sie die Art der lokalen Mailzustellung.

Mail-Transport-Route Konfigurieren Sie hier besondere Transportrouten für Mails abhängig von ihrer Zieladresse.

Mailserverschutz Konfigurieren Sie die SPAM-Schutzeinstellungen des Mailservers. Aktivieren Sie den Virendetektor AMaViS, legen Sie die Art und Intensität der Überprüfung auf SPAM fest und blocken Sie — wenn nötig — die Mailannahme von bestimmten Hosts bzw. Clients komplett.

Mailserver-Weiterleitung Konfigurieren Sie hier, von welchen Netzen aus Ihr Mailserver zum Versenden nicht lokaler Mails genutzt werden darf.

Mail abrufen Konfigurieren Sie die Abholung von Mails von externen Mailboxen über verschiedene Protokolle.

Mailserver-Domains Legen Sie fest, für welche Domains der Mailserver zuständig sein soll. Grundsätzlich muss mindestens eine Hauptdomain konfiguriert sein, wenn Sie den Server nicht als so genannten *null client* konfiguriert haben, der Mails versendet, aber nicht empfängt.

Es werden drei Arten von Domains unterschieden:

main Hauptdomain des lokalen Mailservers

local In lokalen Domains können alle Benutzer Mail bekommen, die auch in der Hauptdomain Mail empfangen können. Im Falle einer Mail an eine lokale Domain wird nur der Teil vor dem @ der Adresse ausgewertet.

virtual In virtuellen Domains bekommen nur solche Benutzer Mails, die eine explizite Adresse in dieser Domain bekommen haben. Virtuelle Mailadressen richten Sie über die YaST Benutzerkonfiguration ein.

2.6.10 Netzwerkdienste (inetd)

Mit diesem Werkzeug können Sie einstellen, welche Netzwerkdienste, z. B. telnet, finger, talk, ftp usw., beim Booten von SUSE LINUX gestartet werden. Sie bewirken, dass sich andere von außen mit Ihrem Rechner über diese Dienste verbinden können. Für jeden Dienst können Sie zudem unterschiedliche Parameter einstellen. Standardmäßig wird der übergeordnete Dienst, der die einzelnen Netzdienste verwaltet (inetd oder xinetd) nicht gestartet.

Nach Start dieses Moduls wählen Sie aus, welchen der beiden Dienste Sie konfigurieren wollen. Im folgenden Dialog entscheiden Sie per Radiobutton, ob inetd (bzw. xinetd) gestartet werden soll. Der (x)inetd Daemon kann mit einer Standardauswahl an Netzwerkdiensten gestartet werden, oder aber Sie stellen eine selbstdefinierte Auswahl an Diensten zusammen, indem Sie der bestehenden Auswahl Dienste 'hinzufügen' oder bestehende 'löschen' bzw. 'bearbeiten'.

Achtung

Konfiguration von Netzwerkdiensten (inetd)

Die Zusammenstellung und Einordnung der Netzwerkdienste auf Ihrem System ist ein komplexer Vorgang, der sehr detaillierte Kenntnis des Konzepts hinter den Linux Netzwerkdiensten erfordert.

Achtung

2.7 Sicherheit und Benutzer

Eine grundlegende Eigenschaft von Linux ist seine Multi-User-Fähigkeit. Daher können mehrere Benutzer unabhängig voneinander an einem einzigen Linux-System arbeiten. Jeder hat seinen eigenen Benutzer-Account, bestehend aus einem Benutzer- bzw. Login-Namen und einem persönlichen Passwort, mit dem er sich am System anmeldet. Dazu kommt außerdem ein persönliches Home-Verzeichnis, in dem die privaten Dateien und Konfigurationen gespeichert werden.

2.7.1 Benutzerverwaltung

Nach dem Aufruf dieses Konfigurations-Tools öffnet sich die Maske Verwaltung von Benutzern und Gruppen. Zunächst können Sie mithilfe der Checkbox festlegen, ob Sie Benutzer oder Gruppen bearbeiten wollen.

YaST bietet Ihnen eine Übersicht über alle lokalen Benutzer auf dem System. Befinden Sie sich in einem größeren Netzwerk können Sie über 'Filter festlegen' alle Systembenutzer (z.B. `root`) oder NIS-Benutzer auflisten lassen. Sie können auch benutzerdefinierte Filtereinstellungen erzeugen. Sie schalten dann nicht mehr zwischen den einzelnen Benutzergruppen um, sondern können diese beliebig kombinieren. Um neue Benutzer anzulegen, klicken Sie auf 'Hinzufügen' und füllen in der Maske die entsprechenden Felder aus. Danach darf sich der neue Benutzer mit seinem Login-Namen und Passwort auf dem Rechner anmelden. Über die Schaltfläche 'Details' nehmen Sie weitere Feineinstellungen für das Benutzerprofil vor. Sie können die Benutzerkennung, das Heimatverzeichnis und die Standard-Login-Shell manuell setzen. Darüber hinaus kann der neue Benutzer hier auch bestimmten Gruppen zugeordnet werden. Die Gültigkeitsdauer des Passworts konfigurieren Sie über 'Passwort-Einstellungen'. Alle diese Einstellungen lassen sich über die Schaltfläche 'Bearbeiten' nachträglich ändern.

Soll ein Benutzer gelöscht werden, selektieren Sie ihn in der Liste und drücken den Button ‘Löschen’.

Für die fortgeschrittene Netzwerkadministration haben Sie die Möglichkeit, über ‘Optionen für Experten’ die Standardeinstellungen für das Anlegen neuer Benutzer zu definieren. Sie legen die Art der Authentifizierung (NIS, LDAP, Kerberos oder Samba) sowie den Algorithmus für die Passwortverschlüsselung fest. Diese Einstellungen sind vor allem für den Einsatz in großen (Firmen-)Netzwerken interessant.

Abbildung 2.16: *Benutzerverwaltung*

2.7.2 Gruppenverwaltung

Starten Sie das Modul Gruppenverwaltung aus dem YaST Kontrollzentrum oder klicken Sie in der Benutzerverwaltung auf die Checkbox ‘Gruppen’. Beide Masken zeigen identische Funktionalität, allerdings legen Sie hier neu Gruppen an, bearbeiten oder löschen sie.

Für eine komfortable Gruppenverwaltung stellt YaST Ihnen eine Liste aller Gruppen zur Verfügung. Soll eine Gruppe gelöscht werden, klicken Sie

diese einfach in der Liste an, so dass die Zeile dunkelblau erscheint, und wählen Sie dann ‘Löschen’. Beim ‘Hinzufügen’ und ‘Bearbeiten’ geben Sie in der zugehörigen YaST Maske Namen, Gruppen-ID (gid) und Mitglieder dieser Gruppe an. Optional könnnen Sie für den Wechsel in diese Gruppe ein Passwort vergeben. Die Filtereinstellungen sind identisch zum Dialog ‘Benutzerverwaltung’.

Abbildung 2.17: *Gruppenverwaltung*

2.7.3 Einstellungen zur Sicherheit

In der Startmaske ‘Lokale Sicherheitskonfiguration’, die Sie unter ‘Sicherheit und Benutzer’ aufrufen, haben Sie die Wahl zwischen vier Optionen: ‘Level 1’ ist für Einzelplatzrechner (vorkonfiguriert), ‘Level 2’ ist für Workstations mit Netzwerk (vorkonfiguriert), ‘Level 3’ ist für Server mit Netzwerk (vorkonfiguriert) und ‘Benutzerdefiniert’ ist für eigene Einstellungen.

Wenn Sie einen der ersten drei Punkte anwählen, haben Sie die Möglichkeit, eine je nach Bedarf entsprechend vorkonfigurierte Systemsicherheit zu übernehmen. Klicken Sie hierfür einfach auf ‘Beenden’. Unter ‘Details’ haben Sie auch Zugang zu den einzelnen Einstellungen, die Sie auf Wunsch

verändern können. Wenn Sie 'Benutzerdefiniert' wählen, gelangen Sie mit 'Weiter' automatisch zu den verschiedenen Dialogen. Hier finden Sie die bei der Installation voreingestellten Werte.

'Passworteinstellungen' Wünschen Sie, dass neue Passwörter vom System geprüft werden, bevor sie übernommen werden, selektieren Sie die beiden Checkboxen 'Überprüfung neuer Passwörter' und 'Plausibilitätstest für Passwörter'. Legen Sie die Mindest- und Maximallänge des Passworts für neu anzulegende Benutzer fest. Ferner legen Sie die Gültigkeitsdauer des Passworts fest und bestimmen, wie viele Tage vor dessen Ablauf der Benutzer beim Login auf der Textkonsole gewarnt werden soll.

'Einstellungen für den Systemstart'
Wie soll die Tastenkombination (Strg)-(Alt)-(Del) interpretiert werden?

Üblicherweise bewirkt sie auf der Textkonsole einen System-Neustart. Das sollten Sie so belassen, es sei denn, Ihr Rechner bzw. Server ist öffentlich zugänglich und Sie befürchten, dass jemand unerlaubt diese Aktion durchführen könnte. Wenn Sie 'Stopp' anwählen, bewirkt diese Tastenkombination ein Herunterfahren des Systems, bei 'Ignorieren' bleibt diese Tastenkombination wirkungslos.

Wer darf das System vom KDM (KDE-Display-Manager – das grafische Login) aus herunterfahren?

'Nur Root' (also der Systemadministrator), 'Alle Benutzer', 'Nobody' oder 'Lokale Benutzer'? Wenn Sie 'Nobody' anwählen, dann kann das System nur noch von der Textkonsole aus heruntergefahren werden.

'Einstellungen für das Anmelden'
Üblicherweise gibt es nach einem fehlgeschlagenen Anmeldeversuch eine Wartezeit von einigen Sekunden, bis eine erneute Anmeldung möglich ist, um das automatische Knacken von Passwörtern zu erschweren. Zudem haben Sie die Möglichkeit, die Punkte 'Aufzeichnung fehlgeschlagener Anmeldeversuche' und 'Aufzeichnung erfolgreicher Anmeldeversuche' zu aktivieren. Falls Sie also Verdacht schöpfen, dass jemand versucht, Ihr Passwort herauszufinden, können Sie die Einträge in den System-Logdateien unter `/var/log` kontrollieren. Über die Checkbox 'Grafische Anmeldung von Remote erlauben' erhalten andere Benutzer über das Netzwerk Zugriff auf Ihren grafischen Anmeldebildschirm. Diese Zugriffsmöglichkeit stellt jedoch ein potentielles Sicherheitsrisiko dar und ist deshalb standardmäßig inaktiv.

'Einstellungen für das Anlegen neuer Benutzer'
Jeder Benutzer hat eine numerische und eine alphanumerische Benutzerkennung. Die Zuordnung geschieht durch die Datei `/etc/passwd` und sollte möglichst eindeutig sein.

Anhand der Daten dieser Maske können Sie festlegen, welche Zahlenbereiche für den numerischen Teil der Benutzerkennung vergeben wird, wenn Sie einen neuen Benutzer anlegen. Das Minimum von 500 für einen Benutzer ist sinnvoll und sollte nicht unterschritten werden. Ebenso verfahren Sie mit den Einstellungen zur Gruppenkennung.

'Verschiedene Einstellungen' Bei 'Einstellung der Dateirechte' gibt es drei Auswahlmöglichkeiten: 'Easy (Einfach)', 'Sicher' und 'Paranoid'. Den meisten Benutzern dürfte Ersteres ausreichen. Der YaST-Hilfetext gibt Ihnen Auskunft über die drei Sicherheitsstufen.

Die Einstellung 'Paranoid' ist extrem restriktiv und kann als Ausgangsbasis für eigene Einstellungen eines Administrators dienen. Wenn Sie 'Paranoid' auswählen, müssen Sie bei der Verwendung von einzelnen Programmen mit Störungen bzw. Fehlfunktionen rechnen, weil Sie nicht mehr die Rechte haben, auf verschiedene Dateien zuzugreifen. Außerdem können Sie in diesem Dialog den Benutzer festlegen, der das Programm updatedb starten soll. Das täglich oder nach dem Booten automatisch ablaufende updatedb erzeugt eine Datenbank (locatedb), in welcher der Ort jeder Datei auf Ihrem Rechner gespeichert wird. Wenn Sie 'Nobody' wählen, kann jeder Benutzer nur Pfade in der Datenbank finden, die auch jeder andere (unprivilegierte) Benutzer sehen würde. Wenn `root` angewählt ist, werden alle lokalen Dateien indiziert, da der Benutzer `root` als Super-User alle Verzeichnisse listen darf.

Zuletzt sollten Sie die Option 'Aktuelles Verzeichnis im Pfad des Benutzers root' deaktivieren.

Mit 'Beenden' schließen Sie Ihre Sicherheitskonfiguration ab.

2.7.4 Firewall

Mit diesem Modul konfigurieren Sie die SuSEfirewall2, um Ihren Rechner vor Angriffen aus dem Internet abzuschirmen. Detaillierte Informationen zur Funktionsweise von SuSEfirewall2 finden Sie in Abschnitt 26.3 auf Seite 705.

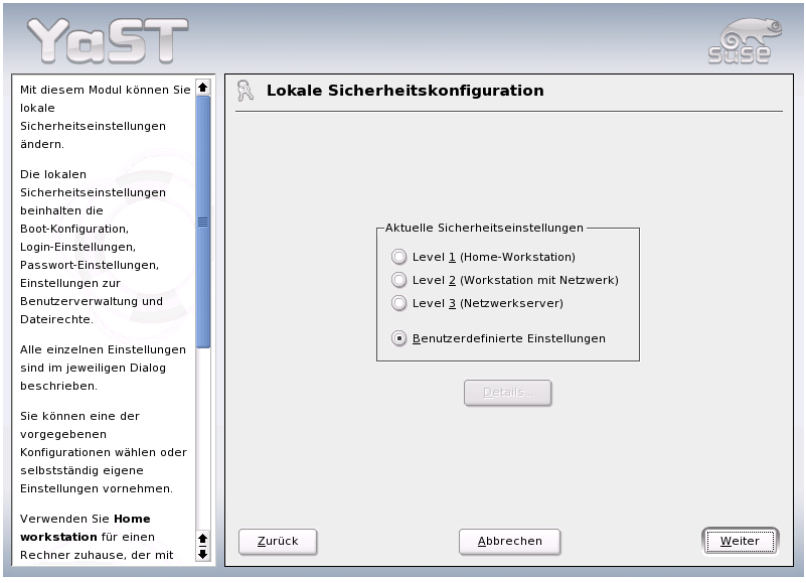

Abbildung 2.18: *YaST: Sicherheitseinstellungen*

2.8 System

Hinweis

S/390, zSeries: Weitere Schritte

Weitere, für IBM S/390 und zSeries relevante Informationen lesen Sie ab Abschnitt 2.8.5 auf Seite 113.

Hinweis

2.8.1 Sicherungkopie der Systembereiche

Mit dem Backup-Modul haben Sie die Möglichkeit, mit YaST Backups Ihres Systems durchzuführen. Das Modul führt keine vollständigen Systembackups durch, sondern sichert nur Informationen über geänderte Pakete, systemkritische Bereiche und Konfigurationsdateien.

Bei der Konfiguration können Sie bestimmen, welche Dateien gesichert werden sollen. Standardmäßig werden Informationen darüber gesichert, welche Pakete sich seit der letzten Installation geändert haben. Zusätzlich können Sie Dateien sichern, die zu keinem Paket gehören, z.B. viele Konfigurationsdateien in Ihrem `/etc`- oder Ihrem `home`-Verzeichnis. Außerdem können kritische Systembereiche auf der Festplatte wie Partitionierungstabellen oder der MBR hinzugefügt werden, die dann bei einer nötigen Restaurierung benutzt werden können.

2.8.2 System wiederherstellen

Mit dem Restore-Modul (Abb. 2.19 auf der nächsten Seite) können Sie Ihr System von einem Backup-Archiv wiederherstellen. Folgen Sie den Anweisungen im YaST. Mit 'Weiter' gelangen Sie in die verschiedenen Dialoge. Zu Beginn geben Sie an, wo sich das/die Archiv(e) befinden, also entweder auf Wechselmedien, auf lokalen Platten oder auf Netzwerk-Filesystemen. Im weiteren Verlauf der Dialoge erhalten Sie zu den Archiven die jeweiligen Beschreibungen und Inhalte und Sie können entscheiden, was Sie aus den Archiven wiederhergestellt haben möchten.

Weiterhin können Sie in zwei Dialogen erstens Pakete zum Deinstallieren wählen, die seit dem letzten Backup neu hinzugekommen sind, und zweitens werden Ihnen Pakete, die seit dem letzten Backup gelöscht wurden, zum erneuten Installieren angeboten. Durch diese beiden zusätzlichen Schritte können Sie exakt den Systemzustand zum Zeitpunkt des letzten Backups wiederherstellen.

Achtung

System wiederherstellen

Da dieses Modul im Normalfall viele Pakete und Dateien installiert, ersetzt oder deinstalliert, sollten Sie es nur benutzen, wenn Sie Erfahrung mit Backups haben, sonst kann Ihnen unter Umständen Datenverlust entstehen.

Achtung

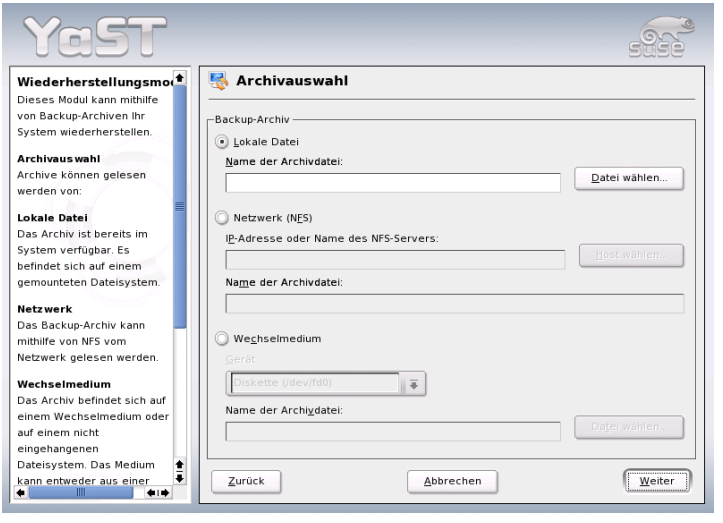

Abbildung 2.19: *YaST: Startfenster des Restore-Moduls*

2.8.3 Erstellen einer Boot-, Rettungs- oder Moduldiskette

Hinweis

S/390, zSeries: Systemrettung

Die hier beschriebene Vorgehensweise ist nicht auf IBM S/390 und zSeries anzuwenden. Eine Beschreibung der Systemrettung auf diesen Plattformen finden Sie im Abschnitt 6.5 auf Seite 208.

Hinweis

Mit diesem YaST-Modul können Sie auf einfache Weise Boot-Disketten, Rettungs-Disketten und Modul-Disketten erstellen. Diese Disketten sind hilfreich, wenn die Boot-Konfiguration in Ihrem System einmal beschädigt sein sollte. Die Rettungs-Diskette ist speziell dann nötig, wenn das Datei-System der Root-Partition beschädigt ist. In diesem Fall wird unter Umständen auch die Modul-Diskette mit verschiedenen Treibern benötigt, um auf das System zuzugreifen (z. B. um ein RAID-System anzusprechen).

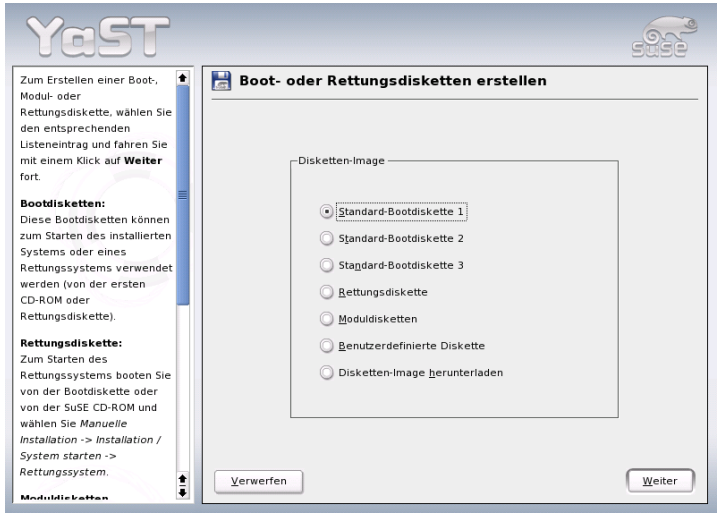

Abbildung 2.20: *Eine Boot-, Rettungs- oder Moduldiskette erstellen*

'Standard-Boot-Diskette' Mit dieser Option erstellen Sie eine Standard-Boot-Diskette, mit der Sie ein bereits installiertes System booten können. Sie wird auch zum Starten des Rettungssystems benötigt.

'Rettungs-Diskette' Diese Diskette entält eine spezielle Umgebung, die es Ihnen ermöglicht, Wartungsarbeiten an Ihrem installierten System durchzuführen, z. B. die Prüfung und Instandsetzung von Datei-Systemen und die Aktualisierung des Bootloaders.

Um das Rettungssystem zu starten, booten Sie zunächst mit der Standard Boot-Diskette und wählen dann 'Manuelle Installation', 'Installation/System starten' und 'Rettungssystem'. Sie werden dann aufgefordert die Rettungs-Diskette einzulegen. Wenn Sie Ihr System für die Nutzung spezieller Treiber konfiguriert haben (z.B. RAID oder USB),

müssen Sie ggf. zusätzlich entsprechende Module von einer Modul-Diskette laden.

'Modul-Disketten' Modul-Disketten enthalten zusätzliche System-Treiber. Der Standard-Kernel unterstützt nur IDE-Laufwerke. Falls die Laufwerke in Ihrem System an spezielle Controller (z.B. SCSI) angeschlossen sind, müssen Sie die entsprechenden Treiber von einer Modul-Diskette laden. Wenn Sie diese Option wählen und auf 'Weiter' klicken, gelangen Sie in einen Dialog zur Erstellung verschiedener Modul-Disketten.

Die folgenden Modul-Disketten sind verfügbar

USB-Module Diese Diskette enthält USB-Module, die z.B. dann gebraucht werden, wenn Sie USB-Laufwerke angeschlossen haben.

IDE-, RAID- und SCSI-Module Weil der Standard-Kernel nur normale IDE-Laufwerke unterstützt, brauchen Sie diese Modul-Diskette, wenn Sie spezielle IDE-Controller benützen. Zusätzlich finden Sie hier alle RAID- und SCSI-Module.

Netzwerk-Module Falls Sie Zugang zu einem Netzwerk benötigen, müssen Sie das passende Treiber-Modul für Ihre Netzwerk-Karte von dieser Diskette laden.

PCMCIA, CDROM (non-ATAPI), FireWire und Dateisysteme Diese Diskette enthält alle PCMCIA-Module, die vor allem bei Laptop-Computern eingesetzt werden. Weiterhin sind hier die Module für FireWire und einige weniger verbreitete Dateisysteme zu finden. Ältere CDROM-Laufwerke, die noch nicht die ATAPI-Norm erfüllen, können mit Treibern von dieser Diskette ebenfalls betrieben werden.

Um Treiber von einer Modul-Diskette in das Rettungssystem zu laden, wählen Sie 'Kernel modules (hardware drivers)' und die gewünschte Modul-Klasse aus (SCSI, Ethernet usw.). Sie werden dann aufgefordert, die entsprechende Modul-Diskette einzulegen, und die enthaltenen Module werden aufgelistet. Wählen Sie dann das gewüschte Modul aus. Achten Sie danach bitte auf die Ausgaben des Systems: 'Loading module <modulename> failed!' ist ein Hinweis darauf, dass die Hardware vom Modul nicht erkannt werden konnte. Manche ältere Treiber benötigen bestimmte Parameter, um die Hardware richtig ansteuern zu können. In diesem Fall sollten Sie die Dokumentation Ihrer Hardware zu Rate ziehen.

'Benutzerdefinierte Diskette' Mit dieser Option können Sie ein beliebiges Disketten-Image von der Festplatte auf eine Diskette schreiben. Die Image-Datei muss bereits vorhanden sein.

'Disketten-Image herunterladen' Hier können Sie nach der Eingabe einer URL und entsprechenden Authentifizierungsdaten ein Disketten-Image aus dem Internet laden.

Um eine der o.g. Disketten zu erzeugen, wählen Sie bitte die entsprechende Option und klicken Sie auf 'Weiter'. Sie werden dann aufgefordert, eine Diskette einzulegen. Nachdem Sie nochmals auf 'Weiter' geklickt haben, wird der Inhalt auf die Diskette geschrieben.

2.8.4 Bootloader-Konfiguration

Hinweis

S/390, zSeries: Bootloader-Konfiguration

Auf den Plattformen IBM S/390 und zSeries wird die Bootloader-Konfiguration mit YaST nicht unterstützt.

Hinweis

Eine detaillierte Beschreibung der Bootloader-Konfiguration mit YaST finden Sie im Abschnitt 8.6 auf Seite 244.

2.8.5 LVM

Der *Logical Volume Manager* (LVM) ist ein Werkzeug zur individuellen Partitionierung der Festplatten mittels logischer Laufwerke. Nähere Informationen zum Thema LVM finden Sie unter Abschnitt 3.10 auf Seite 152.

2.8.6 EVMS

Das *Enterprise Volume Management System*(EVMS) ist, ähnlich wie LVM, ein Werkzeug zur individuellen Partitionierung der Festplatten mittels logischer Laufwerke. Es ist flexibel, erweiterbar und kann durch ein Plug-In Modell an eigene Bedürfnisse für verschiedene Volume Management Systeme angepasst werden.

EVMS ist kompatibel zu bereits bestehenden Speicher- und Volume Management Systemen. Zum Beispiel zählen hierzu DOS-, Linux LVM, GPT-

(engl. *GUID partition table*), S/390-, Macintosh- und BSD-Partitionen u. a. Weitere Informationen erhalten Sie von `http://evms.sourceforge.net`.

2.8.7 Partitionieren

Es ist zwar möglich, im installierten System die Partitionierung zu modifizieren, dies sollten jedoch nur Experten durchführen, die genau wissen, was sie tun, da ansonsten die Gefahr des Datenverlustes sehr hoch ist. Falls Sie das Werkzeug trotzdem benutzen möchten, finden Sie die Beschreibung im Installationsteil dieses Buches im Kapitel 1.7.4 auf Seite 18 (der Partitionierer während der Installation ist der gleiche wie im fertigen System).

2.8.8 Profilmanager (SCPM)

Hinweis

S/390, zSeries: Profilmanager

Dieses Modul ist nicht relevant für SUSE LINUX Enterprise Server auf IBM S/390 und zSeries.

Hinweis

Mit dem Modul für den Profilmanager (engl. *System Configuration Profile Management SCPM*) wurde eine Möglichkeit geschaffen, komplette individuelle Systemkonfigurationen anzulegen, zu verwalten und zwischen ihnen bei Bedarf zu wechseln. Normalerweise kann so etwas vor allem bei mobilen Computern sehr hilfreich sein, die an verschiedenen Standorten (in verschiedenen Netzwerken) und von verschiedenen Personen verwendet werden. Aber auch bei stationären Rechnern können auf diese Weise unterschiedliche Hardwarekomponenten bzw. verschiedene Testkonfigurationen zum Einsatz kommen. Wenn Sie weiterführende Informationen über die Grundlagen und die Bedienung des SCPM erfahren möchten, lesen Sie bitte die entsprechenden Abschnitte im Kapitel 16 auf Seite 361.

2.8.9 Runlevel-Editor

Die Runlevel in SUSE LINUX

SUSE LINUX können Sie in verschiedenen Runleveln betreiben. Standardmäßig startet das System in Runlevel 5. Das bedeutet, Sie haben dann

Mehrbenutzerbetrieb, Netzwerkzugang und grafische Oberfläche (X-Window-System). Als weitere Runlevel haben Sie Mehrbenutzerbetrieb mit Netzwerk ohne X (Runlevel 3), Mehrbenutzerbetrieb ohne Netzwerk (Runlevel 2), Einzelnutzerbetrieb (Runlevel 1 und S), System herunterfahren (Runlevel 0) und System neu starten (Runlevel 6).

Die verschiedenen Runlevel sind hilfreich, wenn in einem höheren Runlevel Probleme mit dem jeweiligen Dienst auftreten (X oder Netzwerk). Dann kann das System in einem niedrigeren Runlevel gestartet werden, um den jeweiligen Dienst zu reparieren. Außerdem laufen viele Server ohne grafische Oberfläche. Deshalb müssen solche Rechner z.B. in den Runlevel 3 gebootet werden.

In der Regel benötigen Sie nur den Standardrunlevel (5). Wenn allerdings Ihre grafische Oberfläche einmal hängen bleiben sollte, können Sie zum Neustart des X-Window-Systems auf eine Textkonsole mit der Tastenkombination Strg-Alt-F1 umschalten, sich dort als Root anmelden und dann in den Runlevel drei schalten mit dem Befehl `init 3`. Damit wird Ihr X-Window-System heruntergefahren und Ihnen steht ausschließlich eine reine Textkonsole zur Verfügung. Starten können Sie es dann einfach wieder mit `init 5`.

Runlevel einstellen im YaST

Bei einer Standardinstallation ist Runlevel 5 ausgewählt. Wollen Sie beim Booten in einen anderen Runlevel starten, können Sie hier einfach den Standardrunlevel ändern. Mit 'Runlevel-Eigenschaften' können Sie außerdem individuell festlegen, welche Dienste in welchem Runlevel gestartet werden.

Achtung

Konfiguration der Runlevels

Fehlerhafte Einstellungen bei Systemdiensten und Runleveln können Ihr System unbrauchbar machen. Informieren Sie sich vor einer Änderung dieser Einstellungen über die möglichen Folgen, um die Funktionsfähigkeit Ihres Systems zu gewährleisten.

Achtung

Weitere Informationen zu Runlevels unter SUSE LINUX finden Sie im Kapitel 11 auf Seite 289.

2.8.10 Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig/` sind die Dateien mit den wichtigsten Einstellungen für SUSE LINUX hinterlegt. Der Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und anschließend in die einzelnen Konfigurationsdateien übernommen werden. Im Allgemeinen ist das manuelle Editieren allerdings nicht notwendig, da bei der Installation eines Paketes oder beim Einrichten eines Dienstes etc. die Dateien automatisch angepasst werden.

Achtung

Systemkonfiguration mit /etc/sysconfig/

Ohne die nötigen Vorkenntnisse sollten Sie keine Änderungen in den Dateien in `/etc/sysconfig/` vornehmen, da sonst die Funktionstüchtigkeit Ihres Systems erheblich beeinträchtigt werden kann.

Achtung

Weitere Informationen zu `/etc/sysconfig/` in SUSE LINUX finden Sie im Kapitel 11 auf Seite 289.

2.8.11 Zeitzone auswählen

Die Zeitzone legen Sie bereits während der Installation fest — hier haben Sie die Möglichkeit, eine nachträgliche Änderung vorzunehmen. Klicken Sie in der Länder-Liste einfach auf Ihr Land und wählen Sie 'Ortszeit' oder 'UTC' (engl. *Universal Time Coordinated*). Bei einem Linux-System ist es üblich, 'UTC' zu verwenden. Rechner mit weiteren Betriebssystemen wie z.B. Microsoft Windows™ verwenden meistens die Ortszeit.

2.8.12 Sprache auswählen

Hier können Sie die Sprache für Ihr Linux-System einstellen, wenn nicht schon während der Installation geschehen.

Die Sprache lässt sich hier auch nachträglich ändern. Die mit YaST vorgenommene Spracheinstellung erstreckt sich systemweit, also für YaST und den Desktop KDE.

2.8.13 Tastaturlayout auswählen

Hinweis

S/390, zSeries: Tastaturlayout

Da IBM S/390 und zSeries über keine lokal angeschlossene Tastatur verfügen, hat dieses Modul für diese Architekturen keine Relevanz.

Hinweis

Hinweis

Konfiguration des Tastaturlayouts

Dieses Modul sollten Sie nur benutzen, wenn Sie auf einem System ohne X-Window-System und grafische Oberfläche arbeiten. Wenn Sie im grafischen System arbeiten (also z.B. mit KDE, sollten Sie die Tastatur, wenn es nötig wird, mit dem Modul 'Anzeige und Eingabegeräte' einrichten; Kapitel 2.4.5 auf Seite 81).

Hinweis

Das gewünschte Tastatur-Layout entspricht in der Regel der gewählten Sprache. Im Testfeld sollten Sie die Einstellung ausprobieren, z.B. ob die Umlaute (ä, ö und ü) korrekt wiedergegeben werden, oder der Buchstabe 'ß' oder das so genannte Pipe-Symbol '|'. Auch die Buchstaben 'z' und 'y' sollten geprüft werden, da diese bei einer amerikanischen Tastatur andersherum liegen.

2.9 Sonstiges

2.9.1 Eine Support-Anfrage stellen

Mit dem Kauf von SUSE LINUX haben Sie Anspruch auf kostenlosen Installationssupport. Informationen hierzu (z. B. über den Umfang, Adresse, Telefonnr. etc.) finden Sie auf unserer Webseite: `http://www.suse.de`

Sie haben aber auch hier in YaST die Möglichkeit, direkt per E-Mail eine Supportanfrage an das SUSE-Team zu stellen. Anspruch darauf haben Sie nach erfolgter Registrierung. Geben Sie bitte zu Beginn die entsprechenden Daten ein – Ihren Registriercode finden Sie auf der Rückseite der CD-Hülle. Zu Ihrer Anfrage selbst wählen Sie bitte im folgenden Fenster die Kategorie

Ihres Problems und schildern Sie es (Abbildung 2.21). Lesen Sie bitte dazu den YaST-Hilfetext. Er gibt Ihnen Auskunft darüber, wie Sie dem Support-Team Ihr Problem am besten beschreiben, so dass es Ihnen helfen kann.

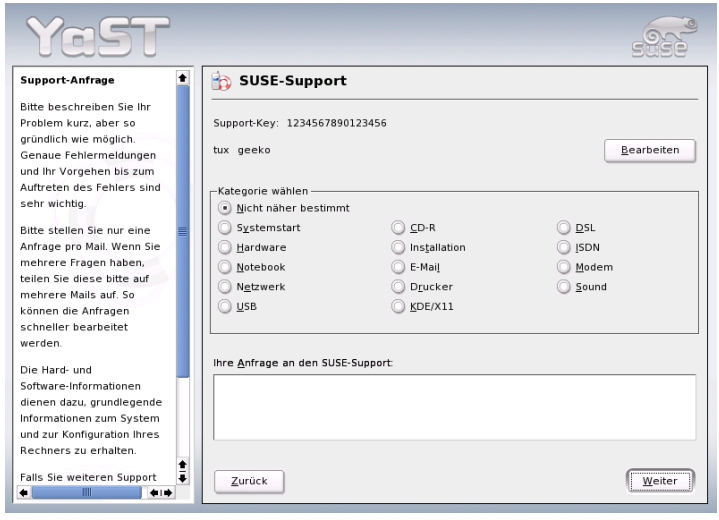

Abbildung 2.21: *Eine Support-Anfrage stellen*

2.9.2 Startprotokoll

Beim Startprotokoll handelt es sich um die Bildschirmmeldungen, die beim Hochfahren des Rechners erscheinen. Das Startprotokoll ist in der Datei `/var/log/boot.msg` hinterlegt. Mit diesem YaST-Modul können Sie es sich komfortabel anzeigen lassen und z.B. nachsehen, ob alle Dienste und Funktionen so gestartet wurden, wie Sie es erwarteten.

2.9.3 Systemprotokoll

Das Systemprotokoll dokumentiert den laufenden Betrieb Ihres Rechners und ist in der Datei `/var/log/messsages` hinterlegt. Sortiert nach Datum und Uhrzeit erscheinen hier die Kernel-Meldungen.

2.9.4 Treiber-CD des Herstellers laden

Mit diesem Modul können Sie Gerätetreiber von einer Linux-Treiber-CD, die Treiber für SUSE LINUX enthält, automatisch installieren.

Falls eine Neuinstallation Ihres SUSE LINUX nötig sein sollte, können Sie nach der Installation mit Hilfe dieses YaST-Moduls die notwendigen Treiber von der Hersteller-CD nachladen.

2.10 YaST im Textmodus (ncurses)

Wenn Sie YaST im Textmodus starten, erscheint zuerst das YaST-Kontrollzentrum (s. Abb. 2.22).

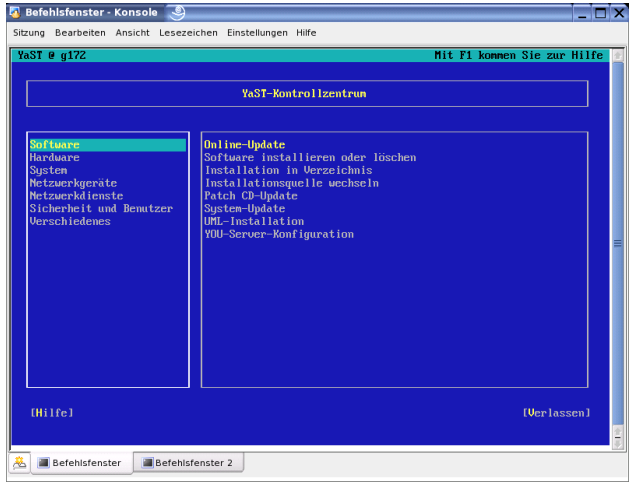

Abbildung 2.22: *Das Hauptfenster von YaST-ncurses*

Sie sehen hier drei Bereiche: In der linken Fensterhälfte, von einem breiten weißen Rahmen umgeben, sind die Kategorien dargestellt, denen die einzelnen Module untergeordnet sind. Die aktive Kategorie ist durch farbige Hinterlegung gekennzeichnet. In der rechten Hälfte sehen Sie, von einem dünnen weißen Rahmen umgeben, einen Überblick über die Module, die in der aktiven Kategorie enthalten sind. Im unteren Fensterbereich liegen die Buttons für ‘Hilfe’ und ‘Verlassen’.

Nach dem ersten Start des YaST-Kontrollzentrums ist automatisch die Kategorie 'Software' selektiert. Die Kategorie wechseln Sie mit den Tasten (↓) und (↑). Zum Start eines Moduls aus der selektierten Kategorie betätigen Sie die Taste (→). Die Modulauswahl erscheint jetzt mit breiter Umrandung. Selektieren Sie das gewünschte Modul über die Tasten (↓) und (↑). Durch andauerndes Drücken der Pfeiltasten „scrollen" Sie durch die Übersicht der verfügbaren Module. Sobald ein Modul selektiert wurde, erscheint der Modultitel farblich hinterlegt. Gleichzeitig wird im unteren Fensterbereich eine kurze Modulbeschreibung eingeblendet.

Über die (Enter) Taste starten Sie das gewünschte Modul. Verschiedene Buttons oder Auswahlfelder im Modul enthalten einen andersfarbigen (bei Standardeinstellungen gelben) Buchstaben. Mit der Kombination (Alt)–(gelberBuchstabe) können Sie den jeweiligen Button ohne umständliche (Tab)-Navigation direkt anwählen.

Das YaST-Kontrollzentrum verlassen Sie, indem Sie den Button 'Verlassen' betätigen oder indem Sie den Unterpunkt 'Verlassen' in der Kategorieübersicht selektieren und (Enter) drücken.

2.10.1 Navigation innerhalb der YaST-Module

Bei der folgenden Beschreibung der Bedienelemente innerhalb der YaST-Module wird davon ausgegangen, dass sämtliche Funktionstasten und (Alt)-Tastenkombinationen funktionieren und nicht systemweit anders belegt wurden. Zu möglichen Ausnahmen lesen Sie bitte Abschnitt 2.10.2 auf Seite 122.

Navigation zwischen Buttons/Auswahllisten
Mit (Tab) und (Alt)–(Tab) oder (Shift)–(Tab) navigieren Sie jeweils zwischen den Buttons und/oder den Rahmen von Auswahllisten hin und her.

Navigation in Auswahllisten In einem aktivierten Rahmen, in dem sich eine Auswahlliste befindet, springen Sie immer mit den Pfeiltasten ((↑) und (↓)) zwischen den einzelnen Elementen, zum Beispiel zwischen den einzelnen Modulen einer Modulgruppe im Kontrollzentrum. Sollten einzelne Einträge innerhalb eines Rahmens über dessen Breite herausragen, „scrollen" Sie mit (Shift)–(→) bzw. (Shift)–(←) horizontal nach rechts und links (alternativ funktioniert auch (Strg)–(e) bzw. (Strg)–(a)). Diese Kombination funktioniert auch dort, wo ein bloßes (→) oder (←) wie im Kontrollzentrum einen Wechsel des aktiven Rahmens bzw. der aktuellen Auswahlliste zur Folge hätte.

Buttons, Radiobuttons und Checkboxen
Die Auswahl von Buttons mit einer leeren eckigen Klammer (Checkbox) oder leerer runder Klammer (Radiobuttons) erfolgt mit (Leertaste) oder (Enter). Alternativ lassen sich Radiobuttons und Checkboxen wie normale Buttons gezielt über (Alt)–(gelberBuchstabe) anwählen. In diesem Fall entfällt die separate Bestätigung mit (Enter). Per Tab-Navigation ist ein separates (Enter) notwendig, damit die ausgewählte Aktion ausgeführt oder der entsprechende Menüpunkt aktiv wird (vgl. Abb. 2.23).

Die Funktionstasten Die F-Tasten ((F1) bis (F12)) sind ebenfalls mit Funktionen belegt. Sie dienen zur schnellen Ansprache der verschiedenen Buttons, die zur Verfügung stehen. Welche F-Tasten mit Funktionen belegt sind, hängt davon ab, in welchem Modul Sie sich im YaST befinden, da in verschiedenen Modulen verschiedene Buttons angeboten sind (z.B. Details, Infos, Hinzufügen, Löschen ...). Für Freunde des alten YaST1 liegen z.B. die Buttons 'OK', 'Weiter' und 'Beenden' auf der Taste (F10). In der Hilfe zu YaST, die Sie mit (F1) erhalten, erfahren Sie die Funktionen hinter den einzelnen F-Tasten.

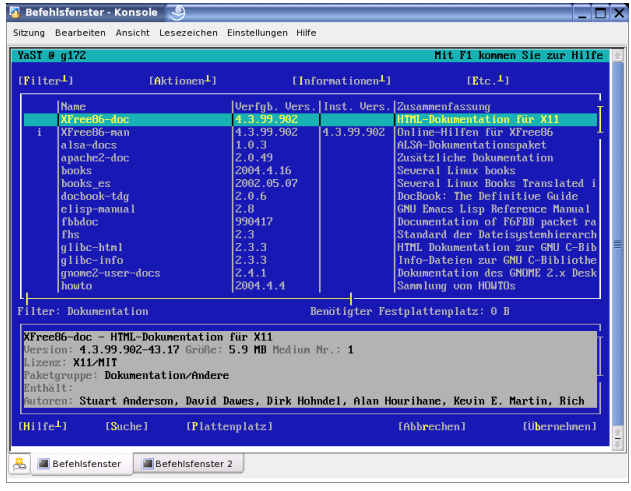

Abbildung 2.23: *Das Modul zur Softwareinstallation*

2.10.2 Einschränkung der Tastenkombinationen

Sollten auf Ihrem System bei laufendem X-Server systemweite (Alt)-Tastenkombinationen bestehen, kann es sein, dass die (Alt)-Kombinationen im YaST nicht funktionieren. Des Weiteren können Tasten wie (Alt) oder (Shift) durch Einstellungen des benutzten Terminals vorbelegt sein.

Ersatz von (Alt) durch (Esc): Alt-Shortcuts können mit (Esc) anstatt (Alt) durchgeführt werden, zum Beispiel ersetzt (Esc)–(h) die Tastenkombination (Alt)–(h).

Ersatz von Vor- und Zurückspringen mittels (Strg)–(f) und (Strg)–(b): Falls (Alt)- und (Shift)-Kombinationen durch den Windowmanager oder das Terminal vorbelegt sind, können Sie hier alternativ die Kombinationen (Strg)–(f) (vorwärts) und (Strg)–(b) (zurück) verwenden.

Einschränkung von Funktionstasten: Auch die F-Tasten sind mit Funktionen belegt. Auch hier können bestimmte F-Tasten durch die Wahl des Terminals vorbelegt sein und daher nicht für YaST zur Verfügung stehen. Auf einer reinen Textkonsole sollten allerdings die (Alt)-Tastenkombinationen und die F-Tasten stets in vollem Umfang verfügbar sein.

2.10.3 Aufruf der einzelnen Module

Zur Zeitersparnis lässt sich jedes der YaST-Module auch einzeln aufrufen. Gestartet werden die Module einfach mit dem Aufruf: `yast modulname`

Das Netzwerkmodul wird zum Beispiel über `yast lan` gestartet. Eine Liste aller Modulnamen, die auf Ihrem System zur Verfügung stehen, erhalten Sie entweder mit dem Aufruf `yast -l` oder über `yast --list`.

2.10.4 Das YaST Online Update

Das YOU-Modul

Das YaST Online Update (YOU) lässt sich wie jedes andere YaST-Modul als `root` von der Kommandozeile aus aufrufen:

```
yast online_update .url <url>
```

`yast online_update` ruft das entsprechende Modul auf. Durch die optionale Angabe von `url` weisen Sie YOU einen Server (lokal oder im Internet) zu, von dem alle Informationen und Patches bezogen werden sollen. Wird diese Angabe nicht beim initialen Aufruf gemacht, wählen Sie den Server/das Verzeichnis über die YaST-Maske aus. Die Bedienung der Maske selbst ist analog der im *Benutzerhandbuch* beschriebenen Bedienung des grafischen YaST-Moduls. Wie bei seinem grafischen Pendant lässt sich auch hier ein per Cronjob automatisiertes Update über den Button 'Vollautomatisches Update konfigurieren' einrichten.

Der Parameter `.cd_default` weist YOU an, von einer Patch-CD zu installieren. Diese Anweisung ist gleichwertig mit `.url cd:///`.

Online Update per Kommandozeile

Über das Kommandozeilentool online_update können Sie Ihr System vollautomatisch, z.B. aus Skripten heraus aktualisieren.

Im konkreten Fall möchten Sie, dass Ihr System regelmäßig zu einer bestimmten Zeit nach Updates auf einem bestimmten Server sucht, die Patches und Patchinformationen herunterlädt, aber noch nicht installiert. Zu einem späteren Zeitpunkt möchten Sie die Menge der Patches sichten und die zu installierenden Patches auswählen:

- Setzen Sie einen Cronjob auf, der folgendes Kommando ausführt:

  ```
  online_update -u <URL> -g <Typangabe>
  ```

  `-u` leitet die Basis-URL des Verzeichnisbaums ein, aus dem die Patches bezogen werden sollen. Es werden die Protokolle `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd` und `dir` unterstützt. Mit `-g` laden Sie die Patches zwar herunter in ein lokales Verzeichnis, installieren Sie aber noch nicht. Optional können Sie die Menge der Patches nach einer der drei Typangaben `security` (sicherheitsrelevante Updates), `recommended` (empfehlenswerte Updates) und `optional` (optionale Updates) filtern. Ohne Filterangabe würde online_update alle verfügbaren neuen Patches des Typs `security` und `recommended`herunterladen.

- Die heruntergeladenen Pakete können Sie anschließend entweder sofort installieren, oder die einzelnen Patches näher untersuchen. Die Patches speichert online_update im Pfad `/var/lib/YaST2/you/mnt/` ab. Rufen Sie, um die Patches abschließend zu installieren, folgenden Befehl auf:

```
online_update -u /var/lib/YaST2/you/mnt/ -i
```

Der Parameter `-u` übergibt die (lokale) URL, unter der die zu installierenden Patches zu finden sind. `-i` startet den Installationsvorgang.

- Möchten Sie die heruntergeladenen Patches vor der Installation sichten und evtl. einzelne verwerfen, rufen Sie die YOU-Maske auf:

  ```
  yast online_update .url /var/lib/YaST2/you/mnt/
  ```

  YOU startet und nimmt als Quelle der Patches statt eines entfernten Verzeichnisses im Internet das lokale Verzeichnis mit den bereits heruntergeladenen Patches. Anschließend selektieren Sie die gewünschten Patches wie bei jeder normalen Installation mittels des Paket-Managers.

Weitere Informationen zu online_update erhalten Sie als Ausgabe des Kommandos `online_update -h`.

Besondere Installationsvarianten

SUSE LINUX lässt sich sehr flexibel installieren. Die Varianten reichen von einer grafischen Schnellinstallation bis zur textbasierten Variante, die zahlreiche manuelle Anpassungen zulässt.

Im Folgenden finden Sie die besonderen Installationsvarianten und Hinweise zur Verwendung unterschiedlicher Installationsquellen (CD-ROM, NFS). In diesem Kapitel finden Sie auch Tipps zu Problemen bei der Installation sowie Anleitungen zu deren Behebung. Den Abschluss bilden ein Abschnitt zur detaillierten Partitionierung und eine Einführung zu SUSE LINUX Enterprise Server auf iSCSI.

3.1 linuxrc 126
3.2 Installation per VNC 136
3.3 Textbasierte Installation mit YaST 137
3.4 SUSE LINUX starten 139
3.5 Besondere Installationen 140
3.6 x86: Tipps und Tricks 141
3.7 x86: ATAPI-CD-ROM bleibt beim Lesen hängen . . 146
3.8 SCSI-Geräte und dauerhafte Gerätedateinamen . . 147
3.9 Partitionieren für Fortgeschrittene 148
3.10 LVM-Konfiguration 152
3.11 Soft-RAID 160
3.12 Massenspeicher über IP-Netzwerke – iSCSI 163

3.1 linuxrc

linuxrc ist ein Programm, das in der Start-Phase des Kernels gestartet wird, bevor richtig gebootet wird. Diese angenehme Eigenschaft des Kernels erlaubt es, einen kleinen modularisierten Kernel zu booten und die wenigen Treiber, die man wirklich braucht, als Module nachzuladen. linuxrc hilft bei Bedarf die relevanten Treiber manuell zu laden. Im Regelfall kann jedoch auf die automatische Hardware-Erkennung vertraut werden, die vor dem Start von YaST durchgeführt wird. Sie können linuxrc nicht nur bei der Installation verwenden, sondern auch als Boot-Tool für ein installiertes System und sogar für ein autonomes (RAM-Disk basiertes) Rettungssystem. Näheres finden Sie in Abschnitt 10.4 auf Seite 280.

3.1.1 Die Grundlage: linuxrc

Mit dem Programm linuxrc können Einstellungen zur Installation vorgenommen werden, sowie notwendige Treiber als Kernelmodule laden werden. Am Ende wird linuxrc YaST starten, und die eigentliche Installation der Systemsoftware und der Programme kann beginnen.

Mit ↑ und ↓ wählen Sie einen Menüpunkt und mit ← und → wählen Sie ein Kommando aus, etwa 'Ok' oder 'Abbruch'. Mit Return wird das Kommando ausgeführt.

Eine genaue Beschreibung von linuxrc finden Sie in Abschnitt 3.1.

Einstellungen

Das Programm linuxrc beginnt automatisch mit der Sprach- und Tastaturauswahl.

- Wählen Sie die Sprache für die Installation aus (zum Beispiel 'Deutsch') und bestätigen Sie mit Return.
- Wählen Sie dann die Tastaturbelegung (zum Beispiel 'Deutsch').

3.1.2 Hauptmenü

Nachdem Sprache und Tastatur eingestellt sind, gelangen Sie in das Hauptmenü von linuxrc (vgl. Abbildung 3.2 auf Seite 128). Normalerweise wird linuxrc benutzt, um Linux zu starten. Ziel ist also der Menüpunkt 'Installation / System starten'. Ob Sie direkt zu diesem Punkt gehen können, hängt von der Hardware des Rechners und dem Installationsvorhaben überhaupt ab. Informationen dazu finden Sie in Abschnitt 3.3 auf Seite 137.

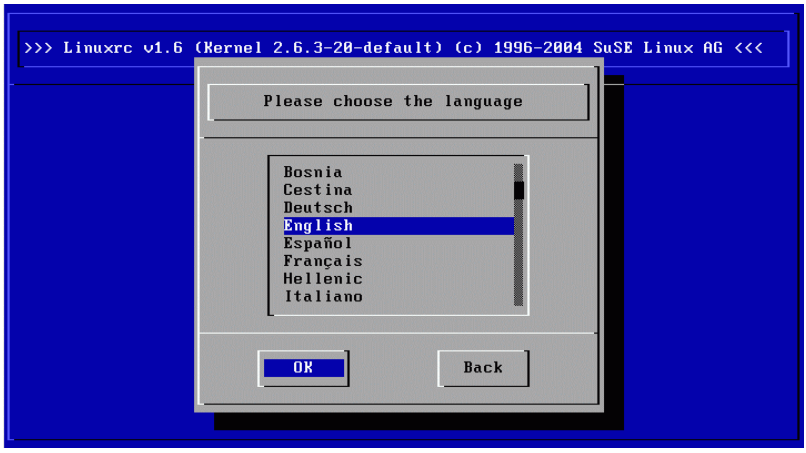

Abbildung 3.1: *Auswahl der Sprache*

3.1.3 System-Information

Unter 'System-Information' (Abbildung 3.3 auf Seite 129) können Sie neben den Meldungen des Kernels auch einige weitere Einzelheiten überprüfen, etwa die I/O-Adressen von PCI-Karten oder die Größe des Hauptspeichers, die von Linux erkannt wurde.

Die folgenden Zeilen zeigen, wie sich eine Festplatte und ein CD-ROM-Laufwerk an einem EIDE-Adapter melden. In diesem Fall müssen Sie keine Kernelmodule für eine Installation laden:

```
hda: IC35L060AVER07-0, ATA DISK drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hdc: DV-516E, ATAPI CD/DVD-ROM drive
ide1 at 0x170-0x177,0x376 on irq 15
hda: max request size: 128KiB
hda: 120103200 sectors (61492 MB) w/1916KiB Cache, CHS=65535/16/63, UDMA(100)
 hda: hda1 hda2 hda3
```

Haben Sie einen Kernel gestartet, der bereits einen SCSI-Treiber fest integriert hat, brauchen Sie natürlich ebenfalls kein SCSI-Modul mehr zu laden. Typische Meldungen bei Erkennung eines SCSI-Adapters und der daran angeschlossenen Geräte sind:

```
SCSI subsystem initialized
scsi0 : Adaptec AIC7XXX EISA/VLB/PCI SCSI HBA DRIVER, Rev 6.2.36
```

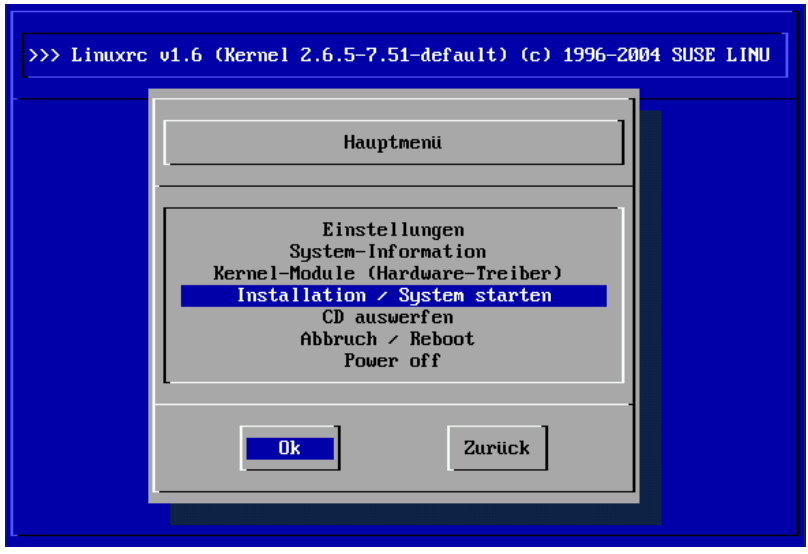

Abbildung 3.2: *Hauptmenü von linuxrc*

```
        <Adaptec aic7890/91 Ultra2 SCSI adapter>
        aic7890/91: Ultra2 Wide Channel A, SCSI Id=7, 32/253 SCBs

(scsi0:A:0): 40.000MB/s transfers (20.000MHz, offset 15, 16bit)
  Vendor: IBM       Model: DCAS-34330W       Rev: S65A
  Type:   Direct-Access                      ANSI SCSI revision: 02
scsi0:A:0:0: Tagged Queuing enabled.  Depth 32
SCSI device sda: 8467200 512-byte hdwr sectors (4335 MB)
SCSI device sda: drive cache: write back
 sda: sda1 sda2
Attached scsi disk sda at scsi0, channel 0, id 0, lun 0
(scsi0:A:6): 20.000MB/s transfers (20.000MHz, offset 16)
  Vendor: TEAC      Model: CD-ROM CD-532S    Rev: 1.0A
  Type:   CD-ROM                             ANSI SCSI revision: 02
```

3.1.4 Laden von Modulen

Hier wählen Sie aus, welche Module (Treiber) Sie benötigen. linuxrc bietet Ihnen die verfügbaren Treiber in einer Liste an. Links sehen Sie den Namen des zuständigen Moduls, rechts eine Kurzbeschreibung der Hardware, für die der Treiber zuständig ist. Für einige Komponenten gibt es mit-

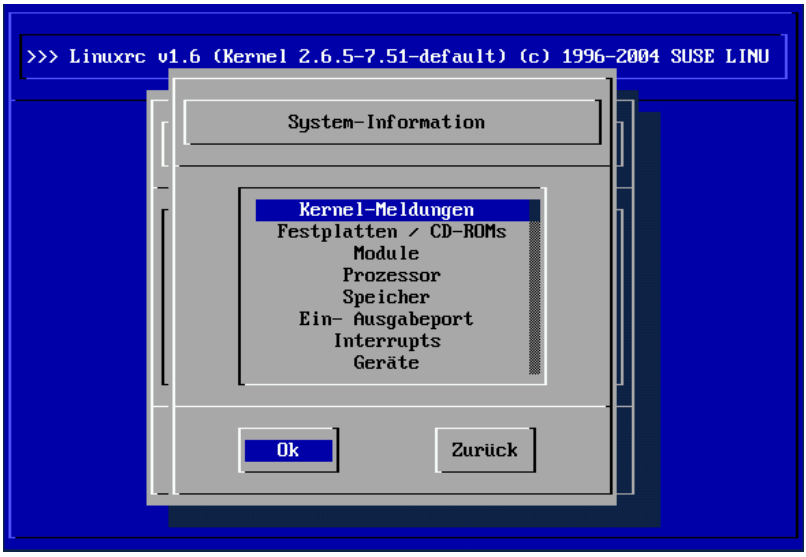

Abbildung 3.3: *Systeminformationen*

unter mehrere Treiber oder neuere Alpha-Treiber. Auch diese werden hier angeboten.

3.1.5 Parametereingabe

Haben Sie den Treiber gefunden, der für Ihre Hardware zuständig ist, drücken Sie (Return). Es erscheint eine Maske, in der Sie etwaige Parameter für das zu ladende Modul eingeben können. Hier sei noch einmal darauf hingewiesen, dass im Gegensatz zur Parametereingabe am Kernel-Prompt mehrere Parameter für das gleiche Modul durch Leerzeichen voneinander getrennt werden müssen.

In vielen Fällen ist die genaue Spezifizierung der Hardware gar nicht notwendig, denn die meisten Treiber finden Ihre Komponenten von alleine. Lediglich bei den Netzwerkkarten und bei älteren CD-ROM-Laufwerken mit eigener Controller-Karte ist die Angabe von Parametern mitunter erforderlich. Probieren Sie es jedenfalls erst einmal mit (Return).

Bei einigen Modulen kann das Erkennen und Initialisieren der Hardware recht lange dauern. Durch Umschalten auf die virtuelle Konsole 4 ((Alt)(F4)) können Sie die Meldungen des Kernels während des Ladens beobachten. Vor allem SCSI-Adapter lassen sich etwas Zeit beim Ladevorgang, da sie

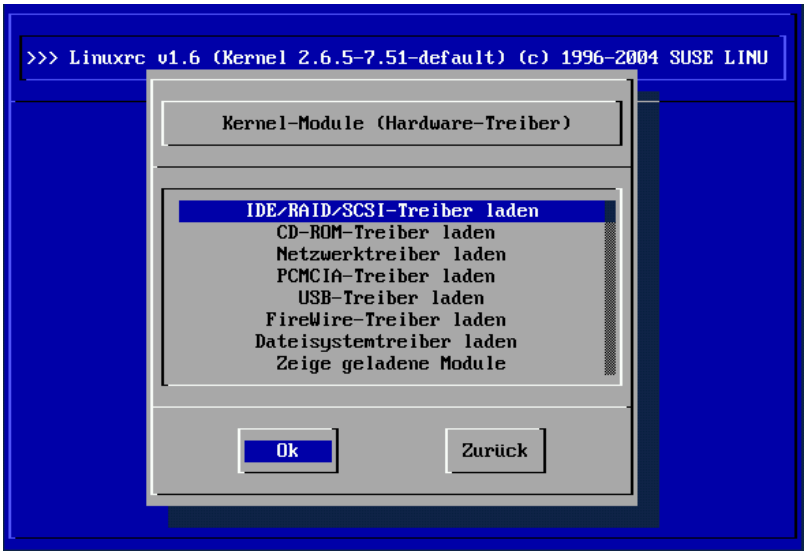

Abbildung 3.4: *Module laden*

eine gewisse Zeit warten, bis sich alle angeschlossenen Geräte gemeldet haben.

Wurde das Modul erfolgreich geladen, werden die Meldungen des Kernels von linuxrc angezeigt, sodass Sie sich vergewissern können, dass alles wie vorgesehen gelaufen ist. Ansonsten weisen die Meldungen möglicherweise auf die Ursache des Scheiterns hin.

Hinweis

Wenn Sie Support für Ihr Installationsmedium (proprietäres CD-ROM-Laufwerk, Parallelport-CD-ROM-Laufwerk, Netzwerkkarte, PCMCIA) unter den Standard-Modulen vermissen, können Sie eventuell auf die zusätzlichen Treiber einer Modul-Diskette zurückgreifen; zum Erstellen einer solchen Diskette vgl. 3.6 auf Seite 141. Gehen Sie bis ans Ende der Liste und wählen Sie dort den Punkt 'Weitere Module'; die Modul-Diskette wird von linuxrc in diesem Fall angefordert.

Hinweis

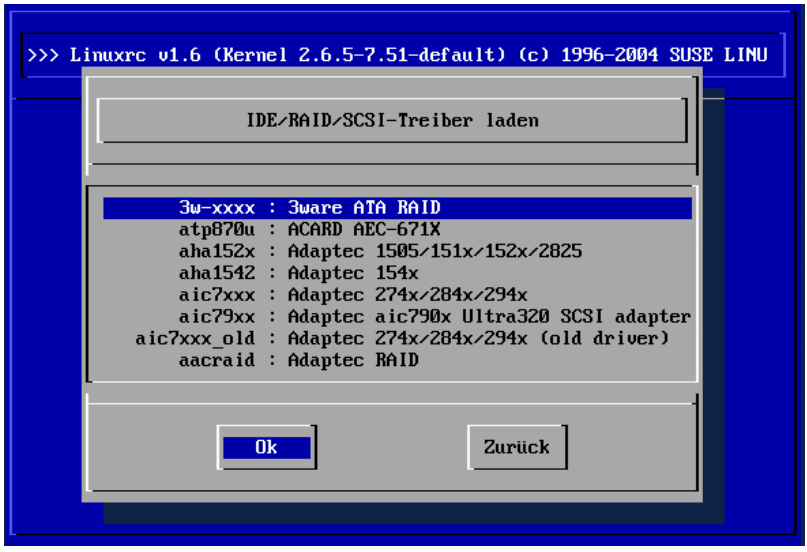

Abbildung 3.5: *Auswahl der SCSI-Treiber*

3.1.6 System / Installation starten

Haben Sie die komplette Kernel-Unterstützung für Ihre Hardware erreicht, können Sie zum Punkt 'System / Installation starten' weitergehen. Von hier aus lassen sich mehrere Vorgänge anstoßen: 'Installation/Update starten', 'Installiertes System booten' (die Rootpartition muss bekannt sein), 'Rettungssystem starten' (vgl. Abschnitt 10.4 auf Seite 280) und 'CD auswerfen'.

Der Punkt 'LiveEval-CD starten' steht nur zur Verfügung, wenn Sie von einer „LiveEval-CD" gebootet haben. ISO-Images können vom FTP-Server heruntergeladen werden (`live-cd-<VERSION>`): `ftp://ftp.suse.com/pub/suse/i386/`

Hinweis

Der Punkt 'LiveEval-CD starten' kann zum Beispiel immer dann nützliche Dienste leisten, wenn man *ohne* eigentliche Festplatten-Installation testen möchte, ob der fragliche Rechner oder das anzuschaffende Notebook kompatibel sind.

Hinweis

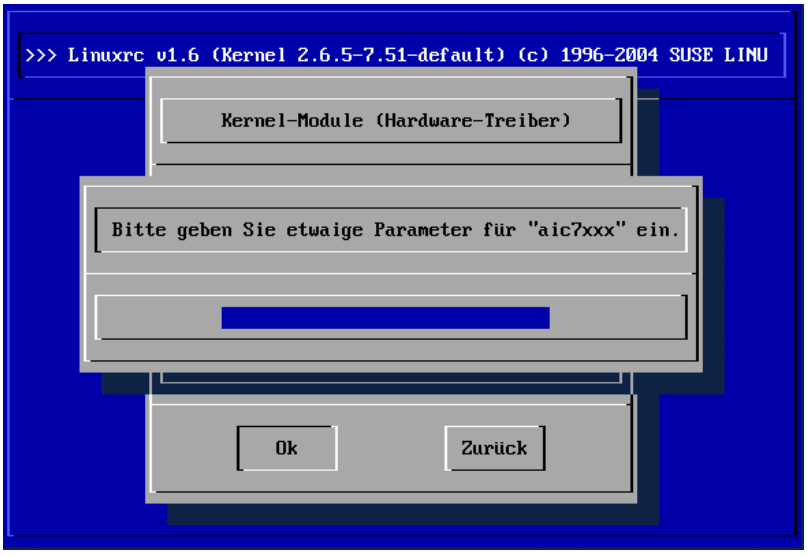

Abbildung 3.6: *Eingabe der Parameter für das Laden eines Moduls*

Zur Installation drücken Sie nun (Return) für den Menüpunkt 'Installation/Update starten'. Dann muss das Quellmedium ausgewählt werden; in der Regel reicht es aus, den Cursor an der Vorauswahl stehen zu lassen: 'CD-ROM'.

Drücken Sie nun (Return). Es wird die Installationsumgebung direkt von der CD 1 bzw. DVD gestartet. Sobald dieser Vorgang abgeschlossen ist, startet YaST und die Installation beginnt.

Für die Installation (Abbildung 3.8 auf Seite 134) und ähnlich auch für das Rettungssystem können Sie verschiedene Quellen wählen (Abbildung 10.1 auf Seite 281).

3.1.7 Mögliche Probleme

linuxrc bietet die gewünschte Tastaturbelegung nicht an.
In einem solchen Fall wählen Sie zunächst eine alternative Belegung (Notnagel: 'English (US)'); nach der Installation kann später auf die genaue Belegung mit YaST umgeschaltet werden.

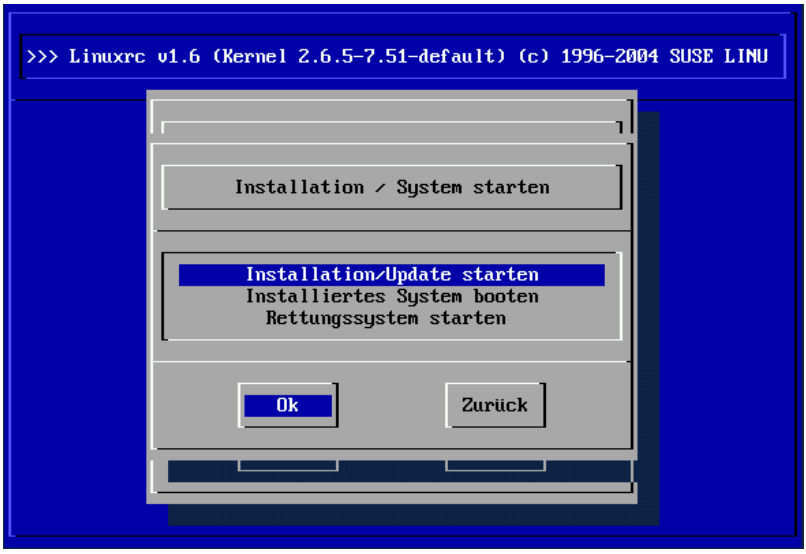

Abbildung 3.7: *Installationsmenü von linuxrc*

Der verwendete SCSI-Adapter wird nicht erkannt:

- Versuchen Sie, das Modul eines kompatiblen Treibers zu laden.
- Prüfen Sie, ob für ihren Adapter eine Treiber-Update Diskette zur Verfügung steht.

Das verwendete ATAPI-CD-ROM-Laufwerk bleibt beim Lesen hängen
Siehe Abschnitt 3.7 auf Seite 146.

System hängt beim Laden der Daten in die RAM-Disk
Unter Umständen kann es zu Problemen beim Laden der Daten in die RAM-Disk kommen, sodass YaST nicht geladen werden kann. Meistens führt der folgende Weg zu einem brauchbaren Ergebnis:

Wählen Sie im linuxrc-Hauptmenü 'Einstellungen' -> 'Debug (Experte)'; dort stellen Sie 'Erzwinge Rootimage' (*Force root image*) auf 'nein'. Gehen Sie zurück ins Hauptmenü und beginnen Sie die Installation erneut.

Abbildung 3.8: Quellmedium in linuxrc auswählen

3.1.8 Parameter an linuxrc übergeben

Befindet sich linuxrc nicht im manuellen Modus, sucht es nach einer Info-Datei, entweder auf Diskette oder in der `initrd` unter `/info`. Erst danach liest linuxrc die Parameter am Kernel-Prompt ein. Die voreingestellten Werte können in der Datei `/linuxrc.config` verändert werden. Diese wird zuerst eingelesen. Allerdings empiehlt es sich Änderungen vorzugsweise in der Info-Datei festzulegen.

Eine Info-Datei besteht aus Schlüsselwörtern und zugehörigen Werten der Form: `key: value`. Diese Schlüssel-Wert-Paare können in der Form `key=value` auch am Boot-Prompt des Installationsmediums übergeben werden. Eine Liste aller Schlüssel finden Sie in der Datei `/usr/share/doc/packages/linuxrc/linuxrc.html`. Einige der wichtigsten werden im Folgenden mit Beispielwerten aufgeführt:

Install: URL (nfs, ftp, hd, ...) Die Installationsquelle mit Hilfe einer `URL` definieren. Zulässige Protokolle sind `cd`, `hd`, `nfs`, `smb`, `ftp`, `http` und `tftp`. Die Syntax enstpricht der gängigen Syntax, wie sie auch in Browsern verwendet werden kann, beispielsweise:

- `nfs://<Server>/<Verzeichniss>`
- `ftp://[Benutzer[:Passwort]@]<Server>/<Verzeichniss>`

Netdevice: eth0 Wenn Sie mehrere Ethernet Devices verfügbar haben, können Sie mit dem Parameter `Netdevice:` das Interface auswählen, das von linuxrc verwendet werden soll.

HostIP: 10.10.0.2 Hiermit wird die IP-Adresse des Rechners festgelegt.

Gateway: 10.10.0.128 Wenn der Installationsserver nicht im gleichen Subnetz wie der Rechner liegt, kann er über den default Gateway erreicht werden.

Proxy: 10.10.0.1 Sie können für die Verbindungstypen ftp und http auch einen Proxy verwenden. Dieser muß über den Parameter `Proxy:` festgelegt werden.

ProxyPort: 3128 Wenn der Proxy nicht den Standard-Port verwendet, kann mit dieser Option der benötigte Port festgelegt werden.

Textmode: 0|1 Verwenden Sie diesen Parameter, um YaST im Textmode zu starten.

AutoYast: ftp://autoyastfile Der Parameter `AutoYast` wird verwendet um eine automatische Installation zu initiieren. Der Wert dieser Option muss eine URL auf eine AutoYast Installationsdatei sein.

VNC: 0|1 Um Rechner, die keine grafische Konsole besitzen, komfortabel installieren zu können, steht Ihnen die Möglichkeit offen, den Installationsprozess per VNC zu kontrollieren. Der Parameter `VNC` aktiviert diesen Dienst auf dem Installationssystem. Vergleichen Sie auch den Parameter `VNCPassword`.

VNCPassword: password Setzt das Passwort um bei einer VNC Installation die Zugriffsberechtigung zu regeln.

UseSSH: 0|1 Stellt einen Zugriff zu linuxrc per SSH bereit. Dies ermöglicht eine Installation mit hilfe des textbasierten YaST

SSHPassword: password Setzt das Passwort für den Benutzer `root` in linuxrc bereit.

Insmod: Modul Parameter Das angegebene Modul in den Kernel laden. Benötigte Parameter zum laden des Moduls werden durch Leerzeichen getrennt übergeben.

AddSwap: 0|3|/dev/hda5 Bei 0 wird nie `swap` angefordert, bei einer positiven Zahl wird die Partition dieser Nummer aktiviert. Alternativ geben Sie den Namen der Partition an.

3.2 Installation per VNC

VNC (*Virtual Network Computing*) ist eine Client-Server Lösung, die es erlaubt einen entfernten X-Server über einen schlanken und leicht zu bedienenden Client zu handhaben. Dieser Client ist für verschiedene Betriebssysteme wie diverse Microsoft Windows Versionen, Apples MacOS und Linux verfügbar.

Der VNC-Client, `vncviewer`, wird eingesetzt, um die grafische Anzeige und die Handhabung von YaST während des Installationsprozesses zu gewährleisten. Vor dem Booten (IPL) des zu installierenden Systems müssen Sie einen entfernten Computer soweit vorbereiten, dass er über das Netz auf das zu installierende System zugreifen kann.

3.2.1 Vorbereitungen zur VNC-Installation

► **S/390, zSeries**
Wie im Handbuch *Architekturspezifika* beschrieben, muss lediglich im Installationsprozess bei IBM S/390 und zSeries die Verbindungsoption `VNC` gewählt werden, damit sich ein beliebiger VNC-Client mit dem Installationssystem verbinden kann und der Installationsprozess mit dem grafischen YaST erfolgen kann. ◄

Um eine VNC-Installation durchzuführen, müssen Sie einige Parameter an den Kernel übergeben. Dies muss vor Starten des Kernels geschehen. Hierzu übergeben Sie am Bootprompt folgende Optionen:

```
vnc=1 vncpassword=<xyz> install=<Quelle>
```

`vnc=1` signalisiert, dass die der VNC-Server auf dem Installationssystem gestartet wird. Mit `vncpassword` übergeben Sie das später zu verwendende Passwort. Die Installationsquelle (`install`) kann entweder manuell angegeben werden (Angabe des Protokolls und URL auf das betreffende Verzeichnis) oder die Anweisung `slp:/` enthalten. Im letzteren Fall wird die Installationsquelle automatisch per SLP-Anfrage ermittelt; weitere Details zu SLP lesen Sie im Abschnitt 21.6 auf Seite 498 nach.

3.2.2 Clients zur VNC-Installation

Die Verbindung zum Installtionsrechner und dem dort laufenden VNC-Server wird über einen VNC-Client hergestellt. Unter SUSE LINUX wird der vncviewer verwendet, der Teil des Paketes `XFree86-Xvnc` ist. Möchten Sie von einem Windows-Client aus Verbindung zum Installationssystem aufbauen, installieren Sie auf dem Windows-System das Programm tightvnc, das Sie auf der ersten CD von SUSE LINUX im Verzeichnis `/dosutils/tightvnc/` finden.

Starten Sie den VNC-Client Ihrer Wahl und geben Sie die IP-Adresse des Installationssystems sowie das VNC-Passwort an, sobald das Programm diese Angaben von Ihnen verlangt.

Alternativ können Sie über einen Java-fähigen Browser ebenfalls VNC-Verbindungen aufbauen. Hierzu geben Sie folgendes in das Adressfeld des Browsers ein:

```
http://<IP-Adresse des Installationssystems>:5801/
```

Ist die Verbindung hergestellt, startet YaST und die Installation kann beginnen.

3.3 Textbasierte Installation mit YaST

Zusätzlich zur Installation mit grafischer Benutzerführung kann das System mithilfe der Textmenüs von YaST installiert werden (Konsolenmodus). Alle YaST-Module stehen auch in diesem Textmodus zur Verfügung. Der Textmodus kann insbesondere dann eingesetzt werden, wenn man keine grafische Oberfläche benötigt (Serversysteme) oder wenn die Grafikkarte von dem X Window System nicht unterstützt wird. Selbstverständlich werden Sehbehinderte, die auf eine textuelle Schnittstelle angewiesen sind, auch diesen Textmodus verwenden.

Zunächst müssen Sie die Bootreihenfolge im BIOS des Rechners so einstellen, dass vom CDROM-Laufwerk gebootet wird. Legen Sie die DVD oder CD 1 in das Laufwerk und starten Sie den Rechner neu. Nach wenigen Augenblicken wird der Startbildschirm angezeigt.

Wählen Sie mit den Tasten ⇧ und ⇩ innerhalb von 10 Sekunden 'Manual Installation', damit *nicht* automatisch YaST gestartet wird. Geben Sie in der Zeile `boot options` Bootparameter ein, falls Ihre Hardware derartige

Parameter verlangt. In der Regel sind jedoch besondere Parameter nicht erforderlich. Mit dem Parameter `textmode=1` erzwingen Sie, dass der Textmodus von YaST benutzt wird. Bei der Eingabe von Text ist zu beachten, dass in dieser frühen Bootphase noch die US-Tastaturbelegung aktiv ist.

Mit der Taste (F2) ('Video mode') legen Sie die Bildschirmauflösung für die Installation fest. Wählen Sie dort 'Text Mode', um in den reinen Textmodus zu gelangen, wenn die Graphikkarte während der Installation sonst Probleme bereitet. Drücken Sie abschließend (Return). Nun erscheint eine Box mit der Fortschrittsanzeige "Loading Linux kernel"; dann bootet der Kernel und linuxrc wird gestartet. Das Programm linuxrc ist menügeführt und wartet auf Eingaben des Benutzers.

Diverse Boot-Schwierigkeiten können in der Regel mit Kernel-Parametern umgangen werden. Für die Fälle, bei denen DMA Schwierigkeiten bereitet, wird die Startoption 'Installation - Safe Settings' angeboten.

Sollte Ihr CD-ROM-Laufwerk (ATAPI) beim Booten des Systems hängenbleiben, lesen Sie bitte den Abschnitt 3.7 auf Seite 146.

Bei Schwierigkeiten mit ACPI (engl. *Advanced Configuration and Power Interface*) stehen die folgenden Kernelparameter zur Verfügung:

`acpi=off` Dieser Parameter schaltet das komplette ACPI-System ab. Dies ist zum Beipiel sinnvoll, wenn Ihr Computer über gar keine ACPI-Unterstützung verfügt oder Sie den konkreten Verdacht haben, dass die ACPI-Implementierung Probleme bereitet.

`acpi=oldboot` Schaltet das ACPI-System fast komplett aus, und nur die Teile, die für das Booten nötig sind, werden verwendet.

`acpi=force` Schaltet ACPI ein, auch wenn Ihr Rechner ein BIOS von vor 2000 hat. Dieser Parameter überschreibt `acpi=off`.

`pci=noacpi` Dieser Parameter schaltet das PCI IRQ-Routing vom neuen ACPI-System aus.

Vgl. auch den SDB-Artikel: `http://portal.suse.de/sdb/de/2002/09/81_acpi.html`

Wählen Sie 'Memory Test' im Bootmenü, um den Speicher zu überprüfen, wenn es beim Laden des Kernels oder im Verlauf der Installation zu „unerklärlichen" Schwierigkeiten kommt. Linux stellt hohe Anforderungen an die Hardware. Der Speicher und dessen Timing müssen einwandfrei eingestellt sein! Mehr Info unter `http://portal.suse.de/sdb/de/2000/11/thallma_memtest86.html`

Lassen Sie den Speichertest am besten über Nacht laufen.

3.4 SUSE LINUX starten

Nach der Installation bleibt die Frage zu klären, wie Sie Linux im täglichen Betrieb starten wollen. In der folgenden Übersicht werden die verschiedenen Alternativen für einen Linux-Start vorgestellt. Welche dieser Startmethoden für Sie die beste ist, hängt vor allem vom Verwendungszweck ab.

Bootdiskette Sie starten Linux über die *Bootdiskette* (Startdiskette). Diese Möglichkeit funktioniert immer und die Bootdiskette kann mit YaST erzeugt werden; vgl. Abschnitt 2.8.3 auf Seite 110.

Die Bootdiskette ist auch eine gute Zwischenlösung, falls Sie beim Einrichten der anderen Möglichkeiten nicht sofort zurechtkommen oder falls Sie die Entscheidung über den endgültigen Bootmechanismus verschieben wollen. Auch wenn Sie den Bootloader eines anderen Betriebssystems nicht überschreiben wollen, ist die Bootdiskette eine brauchbare Lösung.

Linux Bootloader Die technisch sauberste und universellste Lösung ist die Verwendung eines Linux Bootmanagers wie GRUB (GRand Unified Bootloader) oder LILO (LInux LOader), die vor dem Booten die Auswahl zwischen verschiedenen Betriebssystemen zulassen. Der Bootloader kann entweder bereits während der Installation eingerichtet oder später zum Beispiel über YaST konfiguriert werden.

Achtung

Es gibt BIOS-Varianten, die die Struktur des Bootsektors (MBR) überprüfen und nach einer GRUB- oder LILO-Installation fälschlich eine Virus-Warnung ausgeben. Diese Schwierigkeit lässt sich leicht beheben, indem Sie im BIOS die 'Virus Protection' ausschalten, falls diese Option vorhanden ist. Später können Sie sie wieder einschalten. Dieses Feature ist allerdings überflüssig, falls Sie ausschließlich Linux als Betriebssystem verwenden.

Achtung

Eine eingehende Diskussion verschiedener Bootmethoden, insbesondere aber von GRUB und LILO finden Sie in Kapitel 8 auf Seite 223 ff.

3.4.1 Der grafische SUSE-Bildschirm

Auf Konsole 1 der grafische SUSE-Bildschirm dargestellt, wenn als Kernel-Parameter die Option „vga=<wert>“ aktiv ist. Bei der Installation mit YaST wird diese Option automatisch in Abhängigkeit von der gewählten Auflösung und verwendeten Grafikkarte eingetragen.

3.4.2 SUSE-Bildschirm deaktivieren

Prinzipiell haben Sie drei Möglichkeiten:

- Den SUSE-Bildschirm bei Bedarf deaktivieren. Tippen Sie auf der Kommandozeile ein: `echo 0 >/proc/splash`.

  So lässt sich der grafische Bildschirm ausschalten. Durch folgenden Befehl lässt er sich wieder einschalten: `echo 0x0f01 >/proc/splash`.

- Den SUSE-Bildschirm standardmäßig deaktivieren:

  Fügen Sie der Bootloader-Konfiguration einen Kernelparameter `splash=0` hinzu. Im Kapitel 8 auf Seite 223 finden Sie nähere Informationen dazu. Falls Sie ohnehin lieber den Textmodus wünschen, der bei früheren Versionen Standard war, setzen Sie alternativ `vga=normal`.

- Den SUSE-Bildschirm für immer deaktivieren:

  Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option 'Use splash screen instead of boot logo' im Menu 'frame-buffer support'.

  Hinweis

  Wenn Sie im Kernel den Framebuffer-Support deaktiviert haben, ist der Splash-Screen automatisch auch deaktiviert. Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren!

  Hinweis

3.5 Besondere Installationen

3.5.1 Automatische Installation mit Autoyast

Wenn sehr viele gleichartige Rechner installiert werden müssen, bietet es sich an, diese mit Hilfe von Autoyast zu installieren.

Autoyast verwendet die Hardwareerkennung und die Defaulteinstellungen von YaST, kann aber nach eigenen Vorstellungen angepasst werden.

Daher müssen die Rechner nicht alle identisch sein, sondern nur einigermaßen ähnlich sein. Einschränkungen die aufgrund der Hardware bestehen, kann auch autoyast nicht umgehen.

Zu autoyast existiert ein YaST-Modul, mit dem sich ein entsprechendes Konfigurationsfile erstellen lässt. Da die Konfiguration über ein XML-File gemacht wird, kann diese Datei aber auch manuell erstellt oder verändert werden.

Weitere Informationen und eine ausführliche Dokumentation zu autoyast finden Sie in der Dokumentation zum Paket `autoyast2` unter `/usr/share/doc/packages/autoyast2/html/index.html`

3.5.2 Installation via Netzwerk

Um SUSE LINUX über eine Quelle im Netzwerk zu installieren, sind zwei Schritte notwendig:

1. Die zur Installation notwendigen Daten (CDs, DVD) auf einem Rechner verfügbar machen, der später als Installationsquelle agiert.
2. Booten des zu installierenden Systems über Diskette oder CD und Konfiguration des Netzwerkes.

Hinweis

Konfigurieren eines Installations-Servers mit YaST

Detailinformationen zum Aufsetzen eines Installations-Servers und zur Installation der Clients entnehmen Sie Abschnitt 4.1 auf Seite 166.

Hinweis

3.6 x86: Tipps und Tricks

3.6.1 Bootdiskette unter DOS erstellen

Sie brauchen formatierte 3,5 Zoll-HD-Disketten und ein 3,5 Zoll-Disketten-Laufwerk, das bootfähig sein muss.

Auf der CD 1 im Verzeichnis `boot` sind einige Disketten-Abbilder (Images) enthalten. Solch ein Image kann mit geeigneten Hilfsprogrammen auf eine Diskette kopiert werden; die Diskette ist dann eine Bootdiskette.

Die Disketten-Images beinhalten außerdem noch den Loader Syslinux und das Programm linuxrc. Syslinux erlaubt es, während des Bootvorganges den gewünschten Kernel auszuwählen und bei Bedarf Parameter über die verwendete Hardware zu übergeben. Das Programm linuxrc unterstützt Sie beim Laden der Kernelmodule für Ihre spezielle Hardware und startet schließlich die Installation.

Bootdiskette mit rawwritewin erzeugen

Unter Windows steht Ihnen das grafische Programm rawwritewin zur Verfügung. Unter Windows finden Sie dieses Programm auf CD1 im Verzeichnis `dosutils/rawwritewin/`.

Nach dem Start müssen Sie die Image-Datei angeben. Die Image-Dateien liegen ebenfalls auf der CD1 im Verzeichnis boot. Minimal benötigen Sie die Images `bootdisk` und `modules1`. Um diese im Dateibrowser anzuzeigen müssen Sie den Dateityp auf „all files“ ändern.

Legen Sie danach eine Diskette in Ihr Diskettenlaufwerk und klicken Sie auf ‘write’.

Um mehrere Disketten zu beschreiben, wiederholen Sie einfach diese Prozedur.

Bootdiskette mit rawrite erzeugen

Es kommt das DOS-Programm `rawrite.exe` (CD 1, Verzeichnis `dosutils\rawrite` zum Erstellen der SUSE Boot- und Modul-Disketten zum Einsatz. Sie benötigen dazu einen Rechner mit einem DOS (zum Beispiel FreeDOS) oder Windows.

Im Folgenden werden die Schritte beschrieben, falls Sie mit Windows arbeiten:

1. Legen Sie die CD 1 von SUSE LINUX ein.
2. Öffnen Sie ein DOS-Fenster (im Startmenü unter ‘Zubehör’ ->‘MS-DOS-Eingabeaufforderung’).
3. Starten Sie das Programm rawrite.exe mit der richtigen Pfadangabe für das CD-Laufwerk. Im Beispiel befinden Sie sich auf der Festplatte `C:` im Verzeichnis `Windows` und Ihr CD-Laufwerk hat den Buchstaben `D:`

   ```
   C:\Windows: d:\dosutils\rawrite\rawrite
   ```

4. Nach dem Start fragt das Programm nach Quelle (engl. *source*) und Ziel (engl. *destination*) der zu kopierenden Datei. Das ist hier die zum CD-Satz gehörige Bootdiskette, deren Image sich auf CD 1 unter `boot/` befindet. Der Dateiname heißt einfach `bootdisk`. Vergessen Sie auch hier nicht die Pfadangabe für Ihr CD-Laufwerk.

   ```
   C:\Windows: d:\dosutils\rawrite\rawrite
   RaWrite 1.2 - Write disk file to raw floppy diskette

   Enter source file name: d:\boot\bootdisk
   Enter destination drive: a:
   ```

Sobald Sie das Ziellaufwerk `a:` eingegeben haben, fordert Sie rawrite auf, eine formatierte Diskette einzulegen und auf (Enter) zu drücken. Im weiteren Verlauf wird dann der Fortschritt der Kopieraktion angezeigt. Abbruch ist mit der Tastenkombination (Strg)-(C) möglich.

Auf diese Art und Weise können Sie auch die anderen Diskettenimages `modules1`, `modules2`, `modules3` und `modules4` erstellen. Diese werden benötigt, wenn Sie USB- oder SCSI-Geräte bzw. eine Netzwerk- oder PCMCIA-Karte haben und diese während der Installation bereits ansprechen wollen. Eine Moduldiskette kann auch benötigt werden, wenn Sie ein spezielles Dateisystem bereits während der Installation verwenden wollen.

3.6.2 Bootdiskette unter unix-artigem System erstellen

Voraussetzung

Sie können auf ein unix-artiges oder ein Linux-System mit einem funktionstüchtigen CD-ROM-Laufwerk zurückgreifen. Sie brauchen eine geprüfte Diskette (formatiert).

Gehen Sie folgendermaßen vor, um Bootdisketten zu erstellen:

1. Falls Sie die Disketten noch formatieren müssen:

   ```
   fdformat /dev/fd0u1440
   ```

   Mounten Sie die CD 1; zum Beispiel nach `/media/cdrom`:
2. `mount -tiso9660 /dev/cdrom /media/cdrom`
3. Wechseln Sie in das Verzeichnis `boot` auf der CD:

   ```
   cd /media/cdrom/boot
   ```

4. Erstellen Sie die Bootdiskette mit

```
dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
```

In der `LIESMICH`- bzw. der `README`-Datei im `boot`-Verzeichnis erfahren Sie Details zu den Diskettenimages; diese Dateien können Sie mit `more` oder `less` lesen.

Auf diese Art und Weise können Sie auch die anderen Diskettenimages `modules1`, `modules2`, `modules3` und `modules4` erstellen. Diese werden benötigt, wenn Sie USB- oder SCSI-Geräte bzw. eine Netzwerk- oder PCMCIA-Karte haben und diese während der Installation bereits ansprechen wollen. Eine Moduldiskette kann auch benötigt werden, wenn Sie ein spezielles Dateisystem bereits während der Installation verwenden wollen.

Etwas komplexer wird die Angelegenheit, wenn Sie zum Beispiel einen selbstkompilierten Kernel während der Installation verwenden wollen. Schreiben Sie in diesem Fall zunächst das Standard-Image (`bootdisk`) auf die Diskette und überschreiben Sie dann den eigentlichen Kernel (`linux`) mit dem eigenen Kernel (vgl. Abschnitt 9.6 auf Seite 262):

```
dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
mount -t msdos /dev/fd0 /mnt
cp /usr/src/linux/arch/i386/boot/vmlinuz /mnt/linux
umount /mnt
```

3.6.3 Booten von Diskette (SYSLINUX)

Die Bootdiskette kann immer dann zum Einsatz kommen, wenn besondere Anforderungen zum Zeitpunkt der Installation vorliegen (zum Beispiel CD-ROM-Laufwerk nicht verfügbar). Zum Erstellen der Bootdisk vgl. 3.6.1 auf Seite 141 bzw. 3.6.2 auf der vorherigen Seite.

Der Bootvorgang wird von dem Bootloader SYSLINUX (`syslinux`) eingeleitet. SYSLINUX ist so konfiguriert, dass in geringem Umfang eine Hardwareerkennung beim Booten durchgeführt wird. Im Wesentlichen handelt es sich um die folgenden Schritte:

1. Prüfen, ob das BIOS einen Framebuffer gemäß VESA 2.0 unterstützt und den Kernel entsprechend booten.
2. Monitordaten (DDC-Info) auslesen.

3. Den 1. Block von der 1. Festplatte (MBR) lesen, um später bei der Bootloader-Konfiguration die Zuordnung von BIOS-ID zu Linux-Gerätenamen (engl. *Devices*) festzulegen. Dabei wird versucht, den Block über die lba32-Funktionen des BIOS zu lesen, um zu sehen, ob das BIOS diese Funktionen unterstützt.

Hinweis

Wenn beim Start von SYSLINUX (Umschalt) bzw. (Shift) gedrückt ist, werden all diese Schritte übersprungen. Für die Fehlersuche: Man kann in `syslinux.cfg` die Zeile

```
verbose 1
```

einfügen; dann teilt der Bootloader mit, welche Aktion jeweils an der Reihe ist.

Hinweis

Falls der Rechner nicht von Diskette booten will, müssen Sie zuvor möglicherweise die Bootreihenfolge im BIOS des Rechners auf `A,C,CDROM` umstellen.

3.6.4 CD 2 zum Booten verwenden

Zusätzlich zur CD 1 ist auch die zweite CD bootfähig. Während CD 1 über ein bootfähiges ISO-Image arbeitet, wird CD 2 über ein 2.88 MB großes Diskimage gebootet. Verwenden Sie die CD 2 immer dann, wenn Sie genau wissen, dass Sie von CD booten können, das jedoch mit CD 1 nicht funktioniert (Fallback-Lösung).

3.6.5 Unterstützt Linux mein CD-ROM-Laufwerk?

Generell kann man sagen, dass die meisten CD-ROM-Laufwerke unterstützt werden.

- Bei ATAPI-Laufwerken sollte es keine Probleme geben.
- Bei SCSI-CD-ROM-Laufwerken kommt es nur darauf an, ob der SCSI-Controller unterstützt wird, an dem das CD-ROM-Laufwerk angeschlossen ist. In der Komponenten-Datenbank CDB sind die unterstützten SCSI-Controller aufgeführt.

- Auch viele herstellerspezifische CD-ROM-Laufwerke funktionieren mit Linux. In dieser Gruppe kann es gleichwohl zu Problemen kommen. Falls Ihr Laufwerk nicht explizit erwähnt ist, können Sie es immer noch mit einem ähnlichen Typ des gleichen Herstellers versuchen.
- USB CD-ROM-Laufwerke werden ebenfalls unterstützt. Sollte das BIOS Ihres Rechners das Booten von USB-Geräten noch nicht unterstützen, müssen Sie die Installation über Bootdisketten starten. Näheres hierzu finden Sie unter 3.6.3 auf Seite 144. Stellen Sie vor dem Booten von Diskette sicher, dass alle notwendigen USB-Geräte bereits angeschlossen und eingeschaltet sind.

3.7 x86: ATAPI-CD-ROM bleibt beim Lesen hängen

Wenn das ATAPI CD-ROM-Laufwerk nicht erkannt wird oder es beim Lesen hängen bleibt, ist häufig die Hardware nicht korrekt eingerichtet. Normalerweise sollten die einzelnen Geräte am (E)IDE-Bus fortlaufend angeschlossen sein, das heisst das erste Gerät ist Master am ersten Controller, das zweite Slave. Das dritte Gerät schließlich ist Master am zweiten Controller und das vierte dort wieder Slave.

Oft befindet sich in einem Rechner neben der Festplatte nur das CD-ROM-Laufwerk, das als Master am zweiten Controller hängt. Linux kommt in manchen Fällen mit dieser Lücke nicht selbstständig zurecht. Meistens kann dem Kernel durch Angabe eines entsprechenden Parameters aber auf die Sprünge geholfen werden (`hdc=cdrom`).

Gelegentlich ist für ein Laufwerk nur ein falscher Jumper (Brücke) gesetzt; das heißt, es ist als Slave konfiguriert, obwohl es als Master am zweiten Controller angeschlossen ist oder umgekehrt. Im Zweifelsfall sollten diese Einstellungen überprüft und gegebenenfalls korrigiert werden.

Außerdem gibt es noch eine Reihe fehlerhafter EIDE-Chipsätze. Diese sind mittlerweile zum größten Teil bekannt; der Kernel enthält Code, um derartige Probleme zu umgehen. Für diese Fälle existiert ein spezieller Kernel (vgl. das `README` in `/boot` der Installations-CD-ROM).

Sollte das Booten nicht auf Anhieb funktionieren, so versuchen Sie bitte die nachfolgenden Kernelparameter:

hdx=cdrom x steht hier für a, b, c, d etc. und ist folgendermaßen zu lesen:

- a — Master am 1. IDE-Controller
- b — Slave am 1. IDE-Controller
- c — Master am 2. IDE-Controller

Ein Beispiel für einzugebender Parameter ist hdb=cdrom. Mit diesem Parameter geben Sie dem Kernel das CD-ROM-Laufwerk an, falls dieser es nicht findet und Sie ein ATAPI-CD-ROM-Laufwerk haben.

idex=noautotune x steht für 0, 1, 2, 3 etc. und ist folgendermaßen zu lesen:

- 0 — 1. IDE-Controller
- 1 — 2. IDE-Controller

Ein Beispiel für einzugebender Parameter ist hier ide0=noautotune. Dieser Parameter hilft in der Regel bei (E)IDE-Festplatten.

3.8 SCSI-Geräte und dauerhafte Gerätedateinamen

SCSI-Geräte wie z.B. Festplattenpartitionen bekommen beim Booten Gerätedateinamen mehr oder weniger dynamisch zugewiesen. Dies ist solange kein Problem, wie sich an der Zahl oder an der Konfiguation der Geräte nichts ändert. Wenn aber eine weitere SCSI-Festplatte hinzukommt und diese vor der alten Festplatte vom Kernel erkannt wird, dann erhält die alte Platte neue Namen und die Einträge in der Mounttabelle /etc/fstab passen nicht mehr.

Um dies Schwierigkeit zu vermeiden, kann das System Bootskript boot.scsidev verwendet werden. Dieses Skript kann mit Hilfe des Befehls /sbin/insserv aktiviert werden, und benötigte Bootparameter werden in /etc/sysconfig/scsidev abgelegt. Das Skript /etc/rc.d/boot.scsidev richtet daraufhin permanente Gerätenamen im Verzeichnis /dev/scsi/ ein. Diese Gerätenamen können in der Datei /etc/fstab verwendet werden. Wenn persistente Gerätenamen verwendet werden sollen, ist es möglich, in der Datei /etc/scsi.alias diese zu definieren. Vergleichen Sie auch man scsidev.

Hinweis

Gerätenamen und udev

boot.scsidev wird auch unter SUSE LINUX Enterprise Server weiterhin unterstützt. Für SUSE LINUX Enterprise Server sollte jedoch zur Erzeugung von persistenten Gerätenamen möglichst das „user-mode device filesystem“ (udev) verwendet werden. Hierbei werden die Einträge in `/dev/by-id/` von udev vorgenommen.

Hinweis

Im Expertenmodus des Runlevel-Editors ist `boot.scsidev` für die Stufe `B` einzuschalten, dann werden die notwendigen Links in `/etc/init.d/boot.d` angelegt, um die Namen während des Bootens zu erzeugen.

3.9 Partitionieren für Fortgeschrittene

Dieser Abschnitt stellt detaillierte Informationen bereit, anhand derer Sie ein passendes Partitionierungsschema anlegen können. Dies ist insbesondere für diejenigen interessant, die ihr System optimal konfigurieren möchten, sowohl in puncto Sicherheit, als auch was Geschwindigkeit betrifft, und die dafür bereit sind, unter Umständen das bestehende System komplett neu aufzusetzen.

Ein grundlegendes Verständnis der Funktionsweise eines UNIX-Dateisystemes wird vorausgesetzt. Die Begriffe Mountpoint sowie physikalische, erweiterte und logische Partition sollten Ihnen nicht fremd sein.

Überlegen Sie sich zunächst die Antworten auf folgende Fragen:

- Einsatzgebiet dieses Rechners (File-Server, Application-Server, Compute-Server, Einzelplatzrechner)?
- Wie viele Leute werden an diesem Rechner arbeiten (simultane Logins)?
- Wie viele Festplatten hat der Rechner, wie groß sind diese und welches System verwenden sie (EIDE-, SCSI- oder RAID-Controller)?

3.9.1 Die Größe der Swap-Partition

Oft werden Sie lesen: Mindestens doppelt so viel Swap wie Hauptspeicher. Diese Formulierung stammt noch aus einer Zeit, in der 8 MB RAM im Rechner nicht wenig war. Der Rechner soll also über ungefähr 30 bis 40 MB virtuellen Speicher, also Ram plus Swap verfügen. Mit modernen Applikationen müssen auch diese Werte nach oben hin korrigiert werden. Als durchschnittlicher Benutzer ist man auf absehbare Zeit mit 512 MB virtuellem Speicher auf der sicheren Seite. Auf keinen Fall sollten Sie überhaupt keinen Swap-Speicher anlegen.

3.9.2 Partitionierungsvorschläge für spezielle Szenarien

Einsatz als Fileserver

Hier kommt es *wirklich* auf Festplattenperformance an. SCSI-Geräten sollte unbedingt der Vorzug gegeben werden. Achten Sie auch auf Leistungsfähigkeit der Platten und des verwendeten Controllers.

Ein Fileserver bietet die Möglichkeit, Daten zentral zu halten. Hierbei kann es sich um Benutzerverzeichnisse, eine Datenbank oder sonstige Archive handeln. Der Vorteil ist eine wesentlich einfachere Administration. Falls der Fileserver ein größeres Netz bedienen soll (ab 20 Usern), wird die Optimierung des Plattenzugriffs essentiell. Angenommen, Sie möchten einen Linux-Fileserver aufbauen, der 25 Benutzern Heimatverzeichnisse (Home) zur Verfügung stellen soll: Sie wissen, jeder Benutzer wird maximal 100-150 MB für seine persönlichen Daten in Anspruch nehmen. Falls nicht jeder dieser Benutzer stets in seinem Home kompiliert, reicht hierfür eine 4-GB-Partition, welche einfach unter `/home/` gemountet wird.

Haben Sie 50 Benutzer, so wäre rein rechnerisch eine 8-GB-Partition notwendig. Besser ist es in diesem Fall jedoch, `/home/` auf zwei 4-GB-Festplatten aufzuteilen, da diese sich dann die Last (und Zugriffszeit!) teilen.

Hinweis

Den Cache eines Webbrowsers sollten die Benutzer unbedingt auf lokalen Festplatten halten!

Hinweis

Einsatz als Compute-Server

Ein Compute-Server ist in der Regel ein leistungsstarker Rechner, der berechnungsintensive Aufgaben im Netz übernimmt. Solch eine Maschine verfügt typischerweise über einen etwas größeren Hauptspeicher (ab 512 MB RAM). Der einzige Punkt, an dem für einen schnellen Plattendurchsatz gesorgt werden muss, sind etwaige Swap-Partitionen. Auch hier gilt: mehrere Swap-Partitionen auf mehrere Platten verteilen.

3.9.3 Optimierungsmöglichkeiten

Die Platten sind zumeist der begrenzende Faktor. Um diesen Flaschenhals zu umgehen, gibt es drei Möglichkeiten, die am Besten zusammen eingesetzt werden sollten:

- Verteilen Sie die Last gleichmäßig auf mehrere Platten.
- Setzen Sie ein optimiertes Dateisystem ein (zum Beispiel `reiserfs`).
- Statten Sie den Fileserver mit genügend Speicher aus (256 MB Minimum).

Parallelisierung durch mehrere Platten

Die erstgenannte Methode bedarf einer tiefergehenden Erklärung. Die Gesamtzeit, die vergeht, bis angeforderte Daten bereitgestellt werden, setzt sich (in etwa) aus folgenden Teilen zusammen:

1. Zeit, bis die Anforderung beim Plattencontroller ist.
2. Zeit, bis der Plattencontroller diese Anforderung an die Festplatte schickt.
3. Zeit, bis die Festplatte ihren Kopf positioniert.
4. Zeit, bis sich das Medium zum richtigen Sektor gedreht hat.
5. Zeit für die Übertragung.

Punkt 1 ist abhängig von der Anbindung über das Netzwerk und muss dort geregelt werden. Punkt 2 ist eine relativ vernachlässigbare Zeit, die vom Plattencontroller selbst abhängt. Punkte 3 und 4 sind die Hauptbereiche. Gemessen wird die Positionierung in ms. Verglichen mit den in ns gemessenen Zugriffszeiten im Hauptspeicher ist das ein Faktor von einer

Million! Punkt 4 ist von der Drehzahl der Platte abhängig. Auch diese Zeit wird meist mehrere ms betragen. Punkt 5 von der Drehzahl und der Anzahl der Köpfe, ebenso wie von der aktuellen Position des Kopfes (innen oder außen).

Für die optimale Performance sollte man also bei Punkt 3 angreifen. Hier kommt bei SCSI-Geräten das Feature disconnect ins Spiel. Dabei sendet der Controller an das angeschlossene Gerät (in diesem Fall die Festplatte) den Befehl Gehe zu Track x, Sektor y. Nun muss sich die träge Mechanik der Platte in Bewegung setzen. Wenn die Platte intelligent ist (also disconnect beherrscht) und der Treiber für den Controller dieses Feature auch beherrscht, schickt der Controller der Platte unmittelbar daraufhin einen disconnect-Befehl und die Platte trennt sich vom SCSI-Bus ab. Ab jetzt können andere SCSI-Geräte ihre Transfers erledigen. Nach einer Weile (je nach Strategie bzw. Last auf dem SCSI-Bus) wird wieder die Verbindung zur Platte aktiviert. Idealerweise hat diese bereits den geforderten Track erreicht.

In einem Multitasking-Multiuser Betriebssystem wie Linux kann man hier natürlich gut optimieren. Sehen wir uns einen Ausschnitt einer Ausgabe des Befehls `df` an (vgl. Ausgabe 3.1).

Beispiel 3.1: *Beispielausgabe df-Befehl*

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda5 1.8G 1.6G 201M 89% /
/dev/sda1 23M 3.9M 17M 18% /boot
/dev/sdb1 2.9G 2.1G 677M 76% /usr
/dev/sdc1 1.9G 958M 941M 51% /usr/lib
shmfs 185M 0 184M 0% /dev/shm
```

Was bringt uns diese Parallelisierung? Angenommen wir geben in `/usr/src` als Benutzer `root` ein:

```
tar xzf package.tar.gz -C /usr/lib
```

Das soll also package.tar.gz nach `/usr/lib/package` installieren. Hierzu werden von der Shell tar und gzip aufgerufen (befinden sich in `/bin` und somit auf `/dev/sda`), dann wird `package.tar.gz` von `/usr/src` gelesen (befindet sich auf `/dev/sdb`). Als Letztes werden die extrahierten Daten nach `/usr/lib` geschrieben (liegt unter `/dev/sdc`). Sowohl Positionierung, als auch Lesen/Schreiben der platteninternen Puffer können nun quasi parallel ausgeführt werden.

Das ist ein Beispiel von vielen. Als Faustregel gilt, dass bei Vorhandensein entsprechend vieler (gleich schneller) Platten `/usr` und `/usr/lib` auf verschiedenen Platten lagern sollten. Hierbei sollte `/usr/lib` ca. 70 Prozent der Kapazität von `/usr` haben. Das Rootverzeichnis `/` sollte sich bei der Verlagerung auf zwei Platten wegen der Zugriffshäufigkeit auf der Platte mit `/usr/lib` befinden.

Geschwindigkeit und Hauptspeicher

Wir weisen an vielen Stellen darauf hin, dass die Größe des Hauptspeichers unter Linux oft wichtiger ist als die Geschwindigkeit des Prozessors. Ein Grund – wenn nicht sogar der Hauptgrund – ist die Eigenschaft von Linux, dynamische Puffer mit Festplattendaten anzulegen. Hierbei arbeitet Linux mit allerlei Tricks wie read ahead (holt vorsorglich Sektoren im Voraus) und delayed write (spart sich Schreibzugriffe, um sie dann auf einmal auszuführen). Letzteres ist der Grund, warum man einen Linux-Rechner nicht einfach ausschalten darf. Beide Punkte sind dafür verantwortlich, dass sich der Hauptspeicher mit der Zeit scheinbar immer füllt und dass Linux so schnell ist; vgl. auch Abschnitt 10.2.6 auf Seite 273.

3.10 LVM-Konfiguration

YaST bietet ein professionellen Partitioniertool, mit dem Sie bestehende Partitionen bearbeiten, löschen oder neue Partitionen anlegen können. Von diesem YaST-Modul aus gelangen Sie zur Soft-RAID- und LVM-Konfiguration.

Hinweis

Hintergrundinformationen und Tipps zum Partitionieren finden Sie im Abschnitt 3.9 auf Seite 148.

Hinweis

Im Normalfall werden die Partitionen während der Installation festgelegt. Wenn Sie eine zweite Festplatte einbauen wollen, können Sie diese auch im bestehenden Linux-System integrieren. Hierzu ist die neue Festplatte zunächst zu partitionieren, dann müssen die Partitionen gemountet und in die `/etc/fstab` eingetragen werden. Gegebenenfalls ist es nötig, einige Daten umzukopieren, um eine zu kleine `/opt/`-Partition von der alten Festplatte auf die neue zu verschieben.

Wenn Sie die Festplatte, mit der Sie gerade arbeiten, umpartitionieren wollen, ist Vorsicht geboten – grundsätzlich ist dies möglich, danach muss das System aber sofort neu gebootet werden. Unbedenklicher ist es, von der CD zu booten und dann die Umpartitionierung vorzunehmen. Hinter dem Button 'Experten...' im Partitionierer befindet sich ein Popup-Menü mit folgenden Befehlen:

Partitionstabelle neu einlesen Dient dazu, die Partitionierung neu von der Platte einzulesen. Dies benötigen Sie zum Beispiel, wenn Sie die Partitionierung auf der Textkonsole manuell vorgenommen haben.

Mountpunkte von bestehender /etc/fstab übernehmen
Dies ist nur während der Installation relevant. Das Einlesen der alten `fstab` nützt, wenn Sie Ihr System nicht updaten, sondern neu installieren. Dann brauchen Sie die Mountpunkte nicht per Hand eingeben.

Partitionstabelle und Disk-Label löschen
Hiermit überschreiben Sie den alten Partitiontable komplett. Das kann zum Beispiel hilfreich sein, falls Sie Probleme mit ungewöhnlichen Plattenlabels haben sollten. Mit dieser Methode gehen allerdings alle Daten auf der Festplatte verloren.

3.10.1 Logical Volume Manager (LVM)

Ab Kernel Version 2.6 steht Ihnen LVM in der Version 2 zur Verfügung. Dieser ist rückwärtskompatibel zum bisherigen LVM und kann alte Volume-Groups weiterverwalten. Wenn Sie neue Volume-Groups anlegen, müssen Sie entscheiden, ob Sie das neue Format oder die rückwärtskompatible Version verwenden möchten. LVM2 benötigt keine Kernel-Patches mehr, und verwendet den `device-mapper`, der in Kernel 2.6 integriert ist. Beginnend mit diesem Kernel kann LVM nur noch in der Version 2 verwendet werden. In diesem Kapitel ist mit LVM daher immer LVM in der Version 2 gemeint.

Alternativ zu LVM2 können Sie auch EVMS (Enterprise Volume Management System) verwenden. Dieses bietet eine einheitliche Schnittstelle zu Logical Volumes, aber auch zu Raid Volumes. EVMS setzt wie LVM2 auf den Device Mapper in Kernel 2.6 auf.

Der Logical Volume Manager (LVM) ermöglicht Ihnen eine flexible Verteilung des Festplattenplatzes auf die verschiedenen Filesysteme. Da die Partitionen in einem laufenden System nur mit relativ großem Aufwand

geändert werden können, wurde der LVM entwickelt: Er stellt einen virtuellen Pool (Volume Group – kurz VG) an Speicherplatz zur Verfügung, aus dem logische Volumes (LV) nach Bedarf erzeugt werden. Das Betriebssystem greift dann auf diese, statt auf die physikalischen Partitionen zu.

Besonderheiten:

- Mehrere Festplatten/Partitionen können zu einer großen logischen Partition zusammengefügt werden.
- Neigt sich bei einem LV (zum Beispiel `/usr/`) der freie Platz dem Ende zu, können Sie diese bei geeigneter Konfiguration vergrößern.
- Mit dem LVM können Sie sogar im laufenden System Festplatten oder LVs ergänzen. Voraussetzung ist allerdings hot-swap fähige Hardware, die für solche Eingriffe geeignet ist.
- Mehrere Festplatten können im RAID 0 (striping) Modus mit entsprechend verbesserter Performance verwendet werden.
- Das „snapshot"-Feature ermöglicht vor allem bei Servern konsistente Backups während dem laufenden System.

Der Einsatz von LVM lohnt bereits bei umfangreich genutzten Home-PCs oder kleinen Servern. Wenn Sie einen wachsenden Datenbestand haben wie zum Beispiel bei Datenbanken, MP3-Archiven oder Benutzerverzeichnissen etc., dann bietet sich der Logical Volume Manager an. Dann ist es zum Beispiel möglich, Filesysteme zu haben, die größer sind als eine physikalische Festplatte. Ein weiterer Vorteil des LVM ist, dass bis zu 256 LVs angelegt werden können. Beachten Sie jedoch bitte, dass sich die Arbeit mit dem LVM sehr von der mit konventionellen Partitionen unterscheidet.

Anleitung und weiterführende Informationen zur Konfiguration des „Logical Volume Manager" (LVM) finden Sie im offiziellen LVM-Howto `http://tldp.org/HOWTO/LVM-HOWTO/`.

3.10.2 Konfiguration des LVM mit YaST

Die LVM-Konfiguration von YaST wird vorbereitet, indem Sie während der Installation eine LVM-Partition anlegen. Dazu müssen Sie im Vorschlagsbildschirm auf 'Partitionierung' klicken, im folgenden Fenster dann auf 'Verwerfen' oder 'Ändern'. Danach müssen Sie eine Partition für LVM anlegen. Dazu wählen Sie im Partitionierer 'Anlegen' -> 'Nicht formatieren' und dort den Punkt '0x8e Linux LVM'. Die weitere Partitionierung mit

LVM können Sie direkt im Anschluss oder auch später im installierten System vornehmen, indem Sie im Partitionierer die LVM-Partition markieren und dann auf 'LVM...' klicken.

Abbildung 3.9: *YaST: LVM während der Installation aktivieren*

3.10.3 LVM – Partitionierer

Nachdem Sie unter Partitionieren 'LVM...' gewählt haben, kommen Sie in einen Dialog, in dem Sie die Partitionierung Ihrer Festplatten ändern können. Hier können Sie bestehende Partitionen löschen, existierende Partitionen ändern und neue anlegen. Eine Partition, die für LVM verwendet werden soll, muss die Partitionskennung 8E haben. Diese Partitionen sind mit dem Text „Linux LVM“ in der Partitionsliste des Fensters versehen (s. letzter Abschnitt).

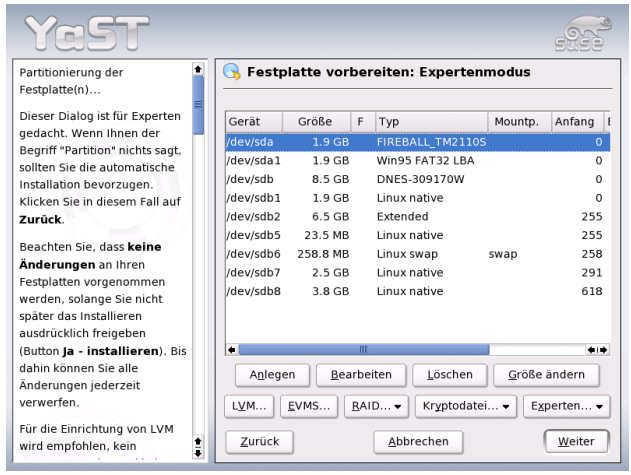

Abbildung 3.10: *YaST: LVM-Partitionierer*

Hinweis

Umpartitionieren von Logical Volumes

Am Anfang der PVs werden Informationen über das Volume in die Partition geschrieben. So „weiß“ eine PV, zu welcher Volume Group das gehört. Wenn Sie neu partitionieren möchten, ist es empfehlenswert, den Anfang dieser Volumes zu löschen. Bei einer Volume Group „system“ und einem Physical Volume „/dev/sda2“ geht das zum Beispiel mit dem Befehl `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`.

Hinweis

Es ist nicht nötig, alle Partitionen, die für LVM vorgesehen sind, einzeln auf die Partitionskennung `8E` zu setzen. YaST setzt die Partitionskennung einer Partition, die einer LVM Volume Group zugeordnet wird, automatisch auf `8E`, wenn dies nötig ist. Wenn auf Ihren Platten unpartitionierte Bereiche vorhanden sind, sollten Sie in diesem Dialog für alle diese Bereiche LVM-Partitionen anlegen. Diese Partitionen sollten Sie sofort auf die Partitionskennung `8E` setzen. Diese müssen nicht formatiert werden, und es kann für sie kein Mountpunkt eingetragen werden.

Falls auf Ihrem System bereits eine gültige LVM-Konfiguration existiert, wird diese bei Beginn der LVM-Konfiguration automatisch aktiviert. Ist

diese Aktivierung erfolgt, kann die Partitionierung aller Platten, die eine Partition enthalten, die zu einer aktivierten Volume Group gehört, nicht mehr verändert werden. Der Linux-Kernel weigert sich, die veränderte Partitionierung einer Festplatte einzulesen, solange auch nur eine Partition dieser Platte benutzt wird.

Eine Umpartitionierung von Platten, die nicht zu einer LVM Volume Group gehören, ist natürlich problemlos möglich. Falls Sie bereits eine gültige LVM-Konfiguration auf Ihrem System haben, ist ein Umpartitionieren normalerweise nicht erforderlich. In dieser Maske müssen Sie nun alle mountpoints konfigurieren, die nicht auf LVM Logical Volumes liegen. Zumindest das Root-Filesystem muss in YaST auf einer normalen Partition liegen. Wählen Sie diese Partition aus der Liste aus und legen Sie sie mit dem Button 'Bearbeiten' als Root-Filesystem fest.

Wir empfehlen aufgrund der größeren Flexibilität von LVM, alle weiteren Filesysteme auf LVM Logical Volumes zu legen. Nach Festlegen der Root-Partition können sie diesen Dialog verlassen.

3.10.4 LVM – Einrichtung der Physical Volumes

Im Dialog 'LVM' werden die LVM Volume Groups (oft mit „VG“ abgekürzt) verwaltet. Wenn auf Ihrem System noch keine Volume Group existiert, werden Sie in einem Popup-Fenster aufgefordert, eine anzulegen. Als Name für die Volume Group auf der sich die Dateien des SUSE LINUX Systems befinden, wird `system` vorgeschlagen.

Die so genannte Physical Extent Size (oft abgekürzt mit PE-Size) bestimmt die maximale Größe eines Physical und Logical Volumes in dieser Volume Group. Dieser Wert wird normalerweise auf 4 Megabyte festgelegt. Dies lässt eine Maximalgröße für ein Physical und Logical Volume von 256 Gigabyte zu. Sie sollten die Physical Extent Size also nur dann erhöhen (zum Beispiel auf 8, 16 oder 32 Megabyte), wenn Sie größere Logical Volumes als 256 Gigabyte benötigen.

In dem folgenden Dialog sind alle Partitionen aufgelistet, die entweder den Type „Linux LVM“ oder „Linux native“ haben. Es werden also keine Swap- und DOS-Partitionen angezeigt. Wenn eine Partition bereits einer Volume Group zugeordnet ist, wird der Name der Volume Group in der Liste angezeigt, nicht zugeordnete Partitionen enthalten die Kennung „--“.

Die gegenwärtig bearbeitete Volume Group kann in der Auswahlbox links oben geändert werden. Mit den Buttons rechts oben ist es möglich, zusätzliche Volume Groups anzulegen und bestehende VGs zu löschen. Es können allerdings nur solche Volume Groups gelöscht werden, denen keine

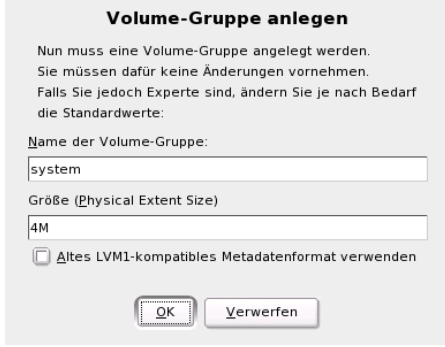

Abbildung 3.11: *YaST: Volume Group anlegen*

Partitionen mehr zugeordnet sind. Für ein normal installiertes SUSE LINUX System ist es nicht nötig, mehr als eine Volume Group anzulegen. Eine Partition, die einer Volume Group zugeordnet ist, wird Physical Volume (PV) genannt.

Um eine bisher nicht zugeordnete Partition der angewählten Volume Group hinzuzufügen, wählen Sie zuerst die Partition an und aktivieren dann den Button 'Volume hinzufügen' unterhalb der Auswahlliste. Daraufhin wird der Name der Volume Group bei der angewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen haben, einer Volume Group zuordnen, sonst bleibt der Platz auf der Partition ungenutzt. Bevor Sie den Dialog verlassen können, muss jeder Volume Group mindestens eine Physical Volume zugeordnet sein.

3.10.5 Logical Volumes

Im diesem Dialog werden die Logical Volumes (oft einfach mit „LV“ abgekürzt) verwaltet.

Logical Volumes sind jeweils einer Volume Group zugeordnet und haben eine bestimmte Größe. Wenn Sie beim Anlegen der Logical Volumes ein Striping Array anlegen möchten, sollten Sie das LV mit den meisten Stripes als erstes anlegen. Ein Striping LV mit n Stripes kann nur dann korrekt angelegt werden, wenn sich der Plattenplatz, der vom LV benötigt wird, noch gleichmäßig auf n Physical Volumes verteilen lässt. Wenn nur zwei PVs zur Verfügung stehen, ist ein LV mit drei Stripes natürlich nicht möglich.

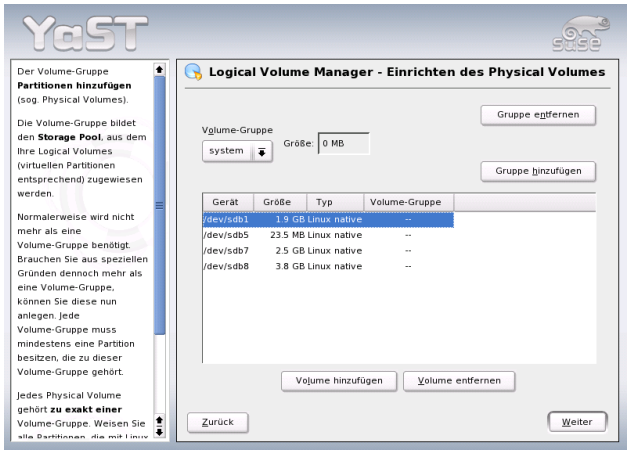

Abbildung 3.12: *YaST: Übersicht über die Partitionen*

Normalerweise wird auf einem Logical Volume ein Filesystem (zum Beispiel reiserfs, ext2) angelegt und ihm ein Mountpunkt zugeordnet. Unter diesem Mountpunkt sind dann im installierten System die Dateien zu finden, die auf diesem Logical Volume gespeichert sind. In der Liste sind alle normalen Linux-Partitionen, denen ein Mountpunkt zugeordnet ist, alle Swap-Partitionen und alle bereits existierenden Logical Volumes eingetragen.

Achtung

Der Einsatz des LVM ist ggf. mit erhöhten Risiken wie zum Beispiel Datenverlust verbunden. Mögliche Gefahren sind Programmabstürze, Stromausfälle oder fehlerhafte Kommandos. Sichern Sie bitte Ihre Daten bevor Sie LVM einsetzen oder Volumes umkonfigurieren – arbeiten Sie also nie ohne Backup!

Achtung

Wenn Sie bereits vorher auf Ihrem System LVM konfiguriert hatten, sind die existierenden Logical Volumes hier eingetragen. Sie müssen diesen Logical Volumes allerdings noch den passenden Mountpunkt zuordnen. Wenn Sie erstmalig auf einem System LVM konfigurieren, existieren in dieser Maske noch keine Logical Volumes und Sie müssen für jeden Mountpunkt ein Logical Volume erzeugen (mit dem Button ‘Hinzufügen’),

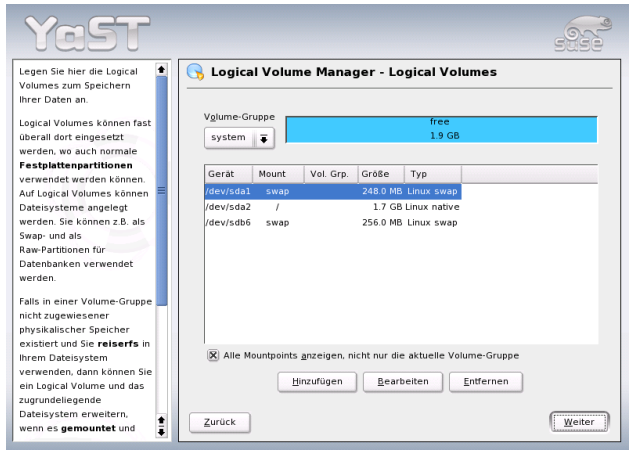

Abbildung 3.13: *YaST: Verwaltung der Logical Volumes*

die Größe, den Filesystem-Typ (zum Beispiel reiserfs oder ext2) und den Mountpunkt (zum Beispiel `/var/`, `/usr/`, `/home/`) festlegen.

Wenn Sie mehrere Volume Groups angelegt haben, können Sie in der Auswahlliste links oben zwischen den einzelnen Volume Groups wechseln. Die angelegten Logical Volumes liegen jeweils in der links oben anzeigten Volume Group. Haben Sie alle Logical Volumes so angelegt, wie sie benötigt werden, ist die LVM-Konfiguration beendet. Sie können den Dialog verlassen und mit der Software-Auswahl fortfahren, falls Sie sich im Installations-Prozess befinden.

3.11 Soft-RAID

Der Sinn von RAID (engl. *Redundant Array of Independent Disks*) ist, mehrere Festplattenpartitionen zu einer großen *virtuellen* Festplatte zu vereinen, um die Performance und die Datensicherheit zu optimieren. Dabei geht das eine jedoch auf Kosten des anderen. Der so genannte *RAID-Level* definiert den Zusammenschluss und die gemeinsame Ansteuerung der Festplatten, die von einem RAID-Controller vorgenommen wird.

Ein RAID-Controller verwendet meist das SCSI-Protokoll, da es gegenüber dem IDE-Protokoll mehr Festplatten besser ansteuern kann und besser für eine parallele Abarbeitung der Befehle geeignet ist.

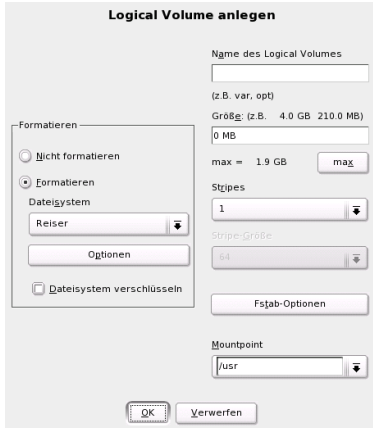

Abbildung 3.14: *YaST: Logical Volumes anlegen*

Statt eines RAID-Controllers, der unter Umständen sehr teuer sein kann, ist auch Soft-RAID in der Lage, diese Aufgaben zu übernehmen. SUSE LINUX bietet Ihnen die Möglichkeit, mit Hilfe von YaST mehrere Festplatten zu einem Soft-RAID-System zu vereinen – eine sehr günstige Alternative zu Hardware-RAID.

3.11.1 Gängige RAID-Level

RAID 0 Dieser Level verbessert die Performance Ihres Datenzugriffs. Im Grunde ist dies gar kein RAID, da es keine Datensicherung gibt, doch die Bezeichnung *RAID 0* hat sich für diese Art von System eingebürgert. Bei RAID 0 schließt man mindestens zwei Festplatten zusammen. Die Performance ist sehr gut – jedoch ist das RAID-System zerstört und Ihre Daten sind verloren, wenn auch nur eine von noch so vielen Festplatten ausfällt.

RAID 1 Dieser Level bietet eine zufrieden stellende Sicherheit für die Daten, weil diese 1:1 auf eine andere Festplatte kopiert werden. Dies nennt man *Festplattenspiegelung* – ist eine Platte zerstört, liegt eine Kopie deren Inhalts auf einer anderen. Es dürfen alle bis auf eine der Festplatten fehlerhaft sein, ohne Daten verloren zu haben. Die Schreibperformance leidet durch den Kopiervorgang ein wenig bei einer Verwendung von RAID 1 (10-20% langsamer), dafür geht der

Lesezugriff deutlich schneller im Vergleich zu einer einzelnen normalen physikalischen Festplatte, weil die Daten doppelt vorhanden sind und somit parallel ausgelesen werden können.

RAID 5 RAID 5 ist ein optimierter Kompromiss aus den beiden anderen Levels was Performance und Redundanz betrifft. Der Festplattenplatz entspricht der Anzahl der eingesetzten Platten minus einer. Die Daten werden wie bei RAID 0 über die Festplatten verteilt. Für die Sicherheit sorgen die *Paritätsblöcke*, die bei RAID 5 auf einer der Partitionen angelegt werden. Diese werden mit XOR miteinander verknüpft – somit lässt sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der Inhalt nach XOR rekonstruieren. Bei RAID 5 ist zu beachten, dass nicht mehr als eine Festplatte gleichzeitig ausfallen darf. Fällt eine aus, muss sie schnellstmöglich ausgetauscht werden, da sonst Datenverlust droht.

3.11.2 Soft-RAID-Konfiguration mit YaST

Zur Soft-RAID-Konfiguration gelangen Sie entweder über ein eigenes 'RAID'-Modul unter 'System' oder über das Partitionierungs-Modul unter 'Hardware'.

1. Schritt: Partitionieren Zunächst sehen Sie unter 'Experten-Einstellungen' im Partitionierungs-Tool Ihre Partitionen aufgelistet. Wenn Sie bereits Soft-RAID-Partitionen angelegt haben, erscheinen diese hier. Andernfalls müssen Sie neue anlegen. Bei RAID 0 und RAID 1 benötigen Sie mindestens zwei Partitionen – bei RAID 1 sind das im Normalfall genau zwei. Für eine Verwendung von RAID 5 hingegen sind mindestens drei Partitionen nötig. Es ist zu empfehlen, nur Partitionen gleicher Größe zu nehmen.

Die einzelnen Partitionen eines RAIDs sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlustes durch den Defekt einer Festplatte bei RAID 1 und 5 verhindert wird bzw. die Performance bei RAID 0 optimiert wird.

2. Schritt: RAID anlegen Wenn Sie auf 'RAID' klicken, erscheint der Dialog, in dem Sie den RAID-Level 0, 1 oder 5 auswählen. In der nächsten Maske haben Sie die Möglichkeit, die Partitionen dem neuen RAID zuzuordnen. Hinter 'Experten-Optionen' finden Sie Einstellmöglichkeiten für die *chunk-size* – hier können Sie Fein-Tuning für die Performance vornehmen. Die Aktivierung der Checkbox 'Persistenter

Superblock' sorgt dafür, dass RAID-Partitionen gleich beim Booten als solche erkannt werden.

Nach Beendigung der Konfiguration sehen Sie auf der Experten-Seite im Partitionierungs-Modul dann das Device `/dev/md0` (etc.) als *RAID* gekennzeichnet.

Troubleshooting Ob eine RAID-Partition zerstört ist, können Sie dem Inhalt der Datei `/proc/mdstats` entnehmen. Grundsätzliche Vorgehensweise in einem Fehlerfall ist es, Ihr Linux-System herunterzufahren und die defekte Festplatte durch eine neue gleichartig partitionierte zu ersetzen. Dann starten Sie Ihr System neu und verwenden den Befehl `raidhotadd /dev/mdX /dev/sdX`. Damit wird die neue Festplatte automatisch in das RAID-System integriert und vollautomatisch rekonstruiert.

Eine Anleitung zur Konfiguration von Soft-RAID und weitere Details hierzu finden Sie im angegebenen Howto:

- `/usr/share/doc/packages/raidtools/Software-RAID-HOWTO.html`
- `http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html`

oder in der Linux-RAID-Mailingliste zum Beispiel über:

- `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`

Dort finden Sie auch Hilfe, falls wider Erwarten komplexe Probleme auftreten sollten.

3.12 Massenspeicher über IP-Netzwerke – iSCSI

Eine zentrale Problematik in Rechenzentren und beim Betrieb von Servern ist die Bereitstellung von Festplattenkapazitäten für Server Systeme. Im Großrechnerbereich wird hierfür häufig Fiber Cannel verwendet, Unix-Rechner und der Großteil der Server werden bisher jedoch meist nicht an zentrale Storage-Lösungen angebunden.

linux-iSCSI stellt eine einfache und verhältnissmäßig billige Lösung zur Verfügung, um Linux Rechner an zentrale Storage Systeme anzubinden.

iSCSI stellt im Prinzip eine Übertragung der SCSI Befehle auf IP-Ebene dar. Wenn ein Programm eine Anfrage auf ein solches Device startet, erstellt das Betriebssystem die erforderlichen SCSI Befehle. Diese werden dann in IP-Pakete eingebettet und bei Bedarf verschlüsselt. Diese Pakete werden dann der entsprechenden iSCSI Gegenstelle übermittelt.

Zur Verwendung von iSCSI benötigen Sie das Paket `linux-iscsi`. Die Verbindungsdaten müssen in der Datei `/etc/iscsi.conf` eingetragen werden. Wenn Sie ein iSCSI Storave Gerät haben, kann diese Konfigurationsdatei zum Beispiel so aussehen:

```
DiscoveryAddress=10.10.222.222
TargetName=iqn.1987-05.com.cisco:00.3b8334455c55.disk1
```

In diesem sehr einfachen Beispiel verwendet das Storage keine Authentifizierung. In `/etc/iscsi.conf` können sehr viele Eigenschaften von iSCSI eingestellt werden. Näheres lesen Sie bitte in der Manual-Page zu iSCSI.

Nach der Konfiguration von iSCSI muss das iSCSI subsystem gestartet werden. Sie erreichen das mit dem Befehl `rciscsi start`. Dabei sollte das System folgende Meldungen ausgeben:

```
rciscsi start
Starting iSCSI: iscsi iscsid fsck/mount                 done
```

Bei der ersten Initialisierung wird die Datei `/etc/initiatorname.iscsi` eingerichtet, mit der sich der Rechner in Zukunft bei dem iSCSI Storage anmeldet. Diese Datei darf nicht einfach kopiert werden. Sie muss für jeden Host neu erzeugt werden.

Wenn der Start erfolgreich war, können Sie an den Systemmeldungen erkennen, welche Devices erkannt wurden. Dies geschieht mit Hilfe des Befehls `dmesg`. Die Verschiedenen Devices stehen nun z.B. unter `/dev/sda` oder `/dev/sdb` zur Verfügung, und können nach belieben Partitioniert und Formatiert werden. Die Mountpoints zu den erkannten Devices sollten in `/etc/fstab.iscsi` eingetragen werden. Diese werden beim Start von iSCSI ausgeführt.

Weitergehende Literatur zu iSCSI finden Sie auf der Webseite des Projektes unter `http://linux-iscsi.sourceforge.net/`

Zentrale Softwareinstallation und -aktualisierung

Wenn Sie innerhalb eines Netzes einen ganzen Pool von Systemen mit SUSE LINUX Enterprise Server installieren möchten, können Sie YaST zur zentralen Bereitstellung der Installationsdaten und zur zentralen Verwaltung von Softwareupdates verwenden.

4.1 Einrichtung eines zentralen Installationsservers . . 166
4.2 Softwareupdates mit dem YOU-Server verwalten . 170
4.3 Booten vom Netz 173

4.1 Einrichtung eines zentralen Installationsservers

Statt jeden einzurichtenden Rechner einzeln mit einem Satz von Installationsmedien zu installieren, können Sie die Installationsdaten auch auf einem dedizierten Installationsserver in Ihrem Netz bereitstellen und für die Installation der Clients von dort beziehen. Der YaST Installationsserver unterstützt HTTP, FTP und NFS. Mit Hilfe des *Service Location Protocols* (SLP) kann dieser Server optional allen im Netz befindlichen Clients bekannt gemacht werden. So entfällt auf den Clients die manuelle Auswahl der Installationsquelle.

Hinweis

Weitere Informationen zu SLP

Detailinformationen zu SLP unter SUSE LINUX erhalten Sie im Abschnitt 21.6 auf Seite 498.

Hinweis

4.1.1 Konfiguration mit YaST

Starten Sie das Modul 'Installation-Server' aus dem Menü 'Verschiedenes' heraus. Der neue Installationsserver wird nun in vier Schritten konfiguriert:

Auswahl des Servertyps YaST unterstützt drei Typen von Installationsservern: HTTP, FTP und NFS. Wählen Sie den Typ des Servers per Radiobutton aus. Der gewählte Serverdienst wird von nun an automatisch bei jedem Hochfahren des Systems gestartet. Wenn auf Ihrem System bereits ein Dienst vom gewählten Typ läuft, den Sie manuell für den Server konfigurieren wollen, deaktivieren Sie die automatische Konfiguration des Dienstes über die Option 'Keine Netzwerkdienste konfigurieren'. Legen Sie in beiden Fällen das Verzeichnis fest, in dem die Installationsdaten auf dem Server bereitgehalten werden sollen (siehe Abbildung 4.1 auf der nächsten Seite).

Detailkonfiguration des gewünschten Servertyps
Dieser Schritt betrifft die automatische Konfiguration der Serverdienste. Bei Deaktivieren der automatischen Konfiguration (s.o.) wird dieser Dialog übersprungen. Legen Sie einen Alias für das

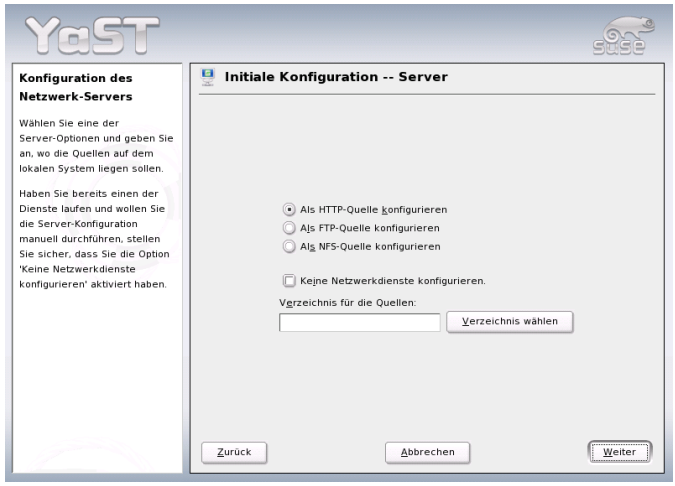

Abbildung 4.1: *YaST Installationsserver: Auswahl des Servertyps*

Wurzelverzeichnis des FTP- oder HTTP-Servers fest, in dem die Installationsdaten zu finden sein werden. Die Installationsquelle wird später unter `ftp://<Server-IP>/<Alias>/<Name>` (FTP) bzw. unter `http://<Server-IP>/<Alias>/<Name>` (HTTP) zu finden sein. ⟨*Name*⟩ steht für den Namen der Installationsquelle, den Sie im folgenden Schritt festlgegen. Sollten Sie im vorangegangenen Schritt NFS gewählt haben, legen Sie Wildcards und `exports` Optionen fest. Der NFS-Server wird unter `nfs://<Server-IP>/<Name>` ansprechbar sein. Details zu NFS und `exports` lesen Sie unter Abschnitt 21.10.4 auf Seite 560 nach.

Konfiguration der Installationsquelle

Bevor die Installationsmedien an ihren Bestimmungsort kopiert werden, legen Sie den Namen der Installationsquelle (idealerweise eine einfach zu merkende Abkürzung aus Produkt- und Versionsbezeichnung) fest. YaST bietet Ihnen die Möglichkeit, statt Kopien der SUSE LINUX CDs ISO-Images der Medien bereitzustellen. Möchten Sie diesen Weg nutzen, aktivieren Sie die entsprechende Checkbox und geben Sie den Verzeichnispfad an, unter dem die ISO-Dateien lokal zu finden sind. Je nachdem, welches Produkt Sie über diesen Installationsserver verteilen möchten, kann es sein, dass Sie weitere Add-on CDs oder Service Pack CDs benötigen, um das Produkt vollständig

zu installieren. Aktivieren Sie die Checkbox 'Nach zusätzlichen CDs verlangen', erinnert Sie YaST automatisch an das Bereitstellen dieser Medien. Wünschen Sie, dass Ihr Installationsserver im Netz per SLP bekanntgegeben wird, aktivieren Sie die entsprechende Checkbox.

Hochladen der Installationsdaten Der langwierigste Teilschritt beim Konfigurieren eines Installationsservers ist das Kopieren der eigentlichen SUSE LINUX CDs. Legen Sie die Medien in der von YaST geforderten Reihenfolge ein und warten Sie das Ende des Kopiervorgangs ab. Sind die Quellen vollständig kopiert, gelangen Sie zurück in den Überblick über die vorhandenen Installationsquellen und schließen die Konfiguration mit der Auswahl von 'Beenden' ab.

Ihr Installationsserver ist nun vollständig konfiguriert und einsatzbereit. Er wird bei jedem Systemstart automatisch mitgestartet. Von Ihrer Seite ist kein manuelles Eingreifen mehr erforderlich. Lediglich dann, wenn Sie im ersten Schritt die automatische Konfiguration des gewählten Netzwerkdienstes durch YaST deaktiviert haben, müssen Sie diesen Dienst per Hand korrekt konfigurieren und starten.

Soll Ihr Installationsserver die Installationsdaten für mehr als ein Produkt oder eine Produktversion bereithalten, starten Sie das YaST Installationsserver-Modul und wählen in der Übersicht (siehe Abbildung 4.2 auf der nächsten Seite) der vorhandenen Installationsquellen 'Konfigurieren', um die neue Installationsquelle zu konfigurieren.

Möchten Sie eine Installationsquelle deaktivieren, wählen Sie im Übersichtsdialog den Button 'Wechseln', um in eine Liste aller verfügbaren Installationsquellen zu gelangen. Selektieren Sie hier den Eintrag, den Sie entfernen wollen und wählen Sie 'Löschen'. Dieser Löschvorgang bezieht sich allerdings lediglich auf das Deaktivieren des Serverdienstes. Die Installationsdaten selbst verbleiben im von Ihnen bestimmten Verzeichnis. Sie können Sie aber von Hand entfernen.

4.1.2 Client-Installation über den Installationsserver

► **S/390, zSeries**
Die Nutzung von NFS- oder FTP- verfügbaren Installationsmedien für die Installation von SUSE LINUX Enterprise Server für IBM S/390 und zSeries wird im Handbuch *Architekturspezifika* im Kapitel *IPL des SUSE LINUX Installationssystems* beschrieben. ◄

Sobald der Installationsserver mit den gewünschten Installtionsdaten im Netz verfügbar ist, können alle im lokalen Netz befindlichen Rechner auf

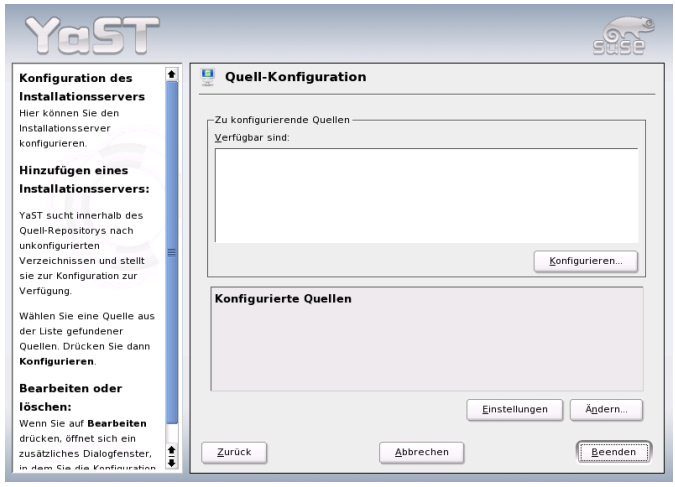

Abbildung 4.2: *YaST Installationsserver: Überblick Installationsquellen*

die Daten zugreifen. Soll ein Client neu installiert werden, benötigen Sie lediglich ein bootfähiges Medium, um den Prozess zu initialisieren. Am Bootprompt geben Sie nun — wie in Kapitel 3.1.8 auf Seite 134 beschrieben — ein, von welchem Server die Installationsdaten zu beziehen sind:

```
install=<URL>
```

Anschließend wird Ihre Netzwerkschnittstelle nach Möglichkeit per DHCP automatisch konfiguriert. Sollte dies nicht möglich sein, konfigurieren Sie sie manuell mit linuxrc oder geben am Bootprompt noch den `HostIP`-Parameter an. Danach wird der Installationskernel gestartet und YaST beginnt mit der Installation. Details zu linuxrc erfahren Sie in Kapitel 3.1 auf Seite 126.

Wird Ihr Installationsserver per SLP im Netz bekanntgegeben, vereinfacht sich die Installationsprozedur:

1. Wählen Sie im grafischen Startbildschirm mit der Funktionstaste (F3) und den Cursortasten die Option `SLP` und bestätigen Sie die Wahl mit (Enter). Oder geben Sie alternativ am Bootprompt `install=slp` ein. In beiden Fällen wird linuxrc eine SLP-Anfrage nach einem Installationsserver im Netz starten.

2. Wählen Sie im Bootmenü nun 'Installation' und bestätigen Sie mit (Enter). Der Installationskernel bootet und YaST beginnt mit der Installation. Sollten per SLP mehrere Installationsquellen zu finden sein, wählen Sie in linuxrc die gewünschte Quelle aus, bevor YaST mit der Arbeit beginnt.

Die weitere Installationsprozedur verläuft wie in den vorangegangenen Kapiteln beschrieben. Detailinformationen zum SLP-Protokoll und seinen Einsatzmöglichkeiten unter SUSE LINUX erhalten Sie im Abschnitt 21.6 auf Seite 498.

4.2 Softwareupdates mit dem YOU-Server verwalten

YaST bietet mit dem 'YOU-Server' Modul die Möglichkeit, einen eigenen lokalen Update-Server einzusetzen, der für alle im Netz befindlichen YOU-Clients stets die aktuellen Softwareupdates bereithält. So wird das Aktualisieren aller im Netz befindlichen Systeme zentralisiert. Der YOU-Server wird entweder manuell oder automatisch gegen einen der von SUSE autorisierten Updateserver im Internet abgeglichen. Je nach Produkt sind dies entweder das SUSE Maintenance Web (`http://sdb.suse.de/download`) oder einer der Mirrors des SUSE FTP-Servers (`ftp://ftp.suse.com/pub/suse`). Die lokalen Clients rufen die Updates via HTTP ab. Der YOU-Server kann so konfiguriert werden, dass er sich per SLP (*Service Location Protocol*) zu erkennen gibt und von allen Clients im Netz automatisch erkannt werden kann.

4.2.1 Konfigurieren des lokalen YOU-Servers

Starten Sie aus dem YaST-Kontrollzentrum das Modul 'Software' → 'YOU-Server-Konfiguration'. Die Dialogmaske ist in drei Teilbereiche gegliedert: Serverkontrolle, Produktliste und Synchronisation.

Der Dialogteil zur 'Server-Steuerung' dient zum Überblick über den Status des YOU-Servers und zur Konfiguration seiner Grundeigenschaften. 'Server starten' startet den YOU-Server. Der Webserver (apache2), der die Updates per HTTP an die untergeordneten Server verteilt, wird nach Auswahl dieses Buttons installiert, konfiguriert und gestartet. Wird die Checkbox 'SLP-Registration' aktiviert, meldet der YOU-Server seinen Dienst am

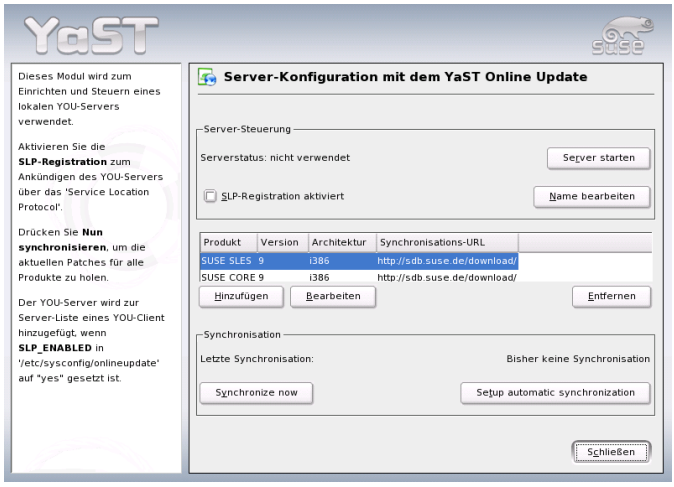

Abbildung 4.3: *Der YOU-Server*

lokalen SLP-Server an. Über den Button ‘Name ändern’ können Sie die Bezeichnung, unter der Ihr Ihr lokaler YOU-Server bei den YOU-Clients erscheint, ändern.

Die Produktliste zeigt die Namen aller Produkte an, für die der YOU-Server aktuell Updates bereithält und von welchem URL die Updates bezogen werden. Standardmäßig wird jenes Produkt angezeigt, das auf der Maschine läuft, auf der der Server eingerichtet wird. Mit den Buttons ‘Hinzufügen’, ‘Ändern’ und ‘Löschen’ bearbeiten Sie die Produktliste. ‘Hinzufügen’ und ‘Ändern’ rufen einen Dialog auf, in dem Produktname, Hardware-Architektur, Version und Herkunfts-URL eingetragen werden. Bei Updateservern, die eine Authentifizierung erfordern (SUSE Maintenance Web) tragen Sie in diesem Dialog Benutzername und Passwort ein.

Hinweis

Produktdaten

Produktname, Version und Architekturbezeichnung der Hardware werden von YOU intern dazu verwendet, den Pfad, unter dem die Updates auf dem Quellserver gesucht werden, zu bilden. Bitte stellen Sie sicher, dass hier die korrekten Bezeichnungen verwendet werden, da YOU sonst die gewünschten Updates auf dem Quellserver nicht finden kann. Sie erhalten die Daten entweder über den YOU-Client-Dialog oder durch Eingabe von `online_update -c` auf der Kommandozeile.

Hinweis

Im Synchronisations-Teilbereich wird der Status der Synchronisation mit dem Quellserver bzw. das Datum des letzten Synchronisationsvorgangs angezeigt. Mit dem Button 'Jetzt synchronisieren' lösen Sie einen Synchronisationsvorgang aus. Alle Updates für die gelisteten Produkte werden heruntergeladen und unter `/var/lib/YaST2/you/mnt/` abgelegt. Von hier aus werden die Updates via HTTP allen angegliederten YOU-Clients zum Installieren angeboten. Über den Button 'Automatische Synchronisierung konfigurieren' rufen Sie einen Dialog auf, in dem Sie die Synchronisation mittels eines Cronjobs bequem automatisieren können.

4.2.2 Konfigurieren der Clients

Die lokalen YOU-Clients, die Sie über 'YaST-Kontrollzentrum' → 'Online-Update' aufrufen, konfigurieren Sie entweder manuell so, dass sie die Updates von Ihrem YOU-Server beziehen oder nutzen die SLP-Funktionaltät von YaST, um die Serveradresse automatisch zu ermitteln.

manuelle Konfiguration Geben Sie im URL-Feld des YOU-Clients den URL ein, der auf Ihren lokalen Server weist: `http://<servername>/YOU` oder tragen Sie alternativ in `/etc/youservers` diesen Pfad ein.

Serversuche via SLP Aktivieren Sie die SLP-Suche auf Ihrem YOU-Client, indem Sie in der Datei `/etc/sysconfig/onlineupdate` die Variable `SLP_ENABLED` auf `yes` setzen.

Die Clients können per Cronjob so konfiguriert werden, dass Sie regelmäßig den lokalen Server nach Updates durchsuchen. Alternativ können Sie den Updatevorgang manuell auslösen. Eine Beschreibung des YOU-Clients finden Sie unter Abschnitt 2.3.2 auf Seite 54.

4.3 Booten vom Netz

Um mit einer bootfähigen Netzwerkkarte das System zu booten, benötigen Sie drei Dienste:

1. Sie benötigen einen Dienst, der die Anfrage der Netzwerkkarte beantwortet. Bei Intel-basierten Rechnern ist dies im Allgemeinen PXE. Bei dem PXE Bootvorgang wird zunächst ein spezielles PXE Bootimage geladen, das die weitere Steuerung des Bootvorgangs übernimmt. Itanium Processor Family Rechner werden zum Netzwerkboot über elilo gestartet.
2. Der Kernel und das erste System werden von tftpd zur Verfügung gestellt. Zur Konfiguration des tftpd steht Ihnen ein YaST-Modul zur Verfügung.
3. Wenn Sie mit dem Bootserver zur Installation booten möchten, dann benötigen sie als dritten Dienst einen Installationsserver. Dieser Dienst wird in Abschnitt 4.1 auf Seite 166 ausführlich beschrieben.
4. Mit Hilfe dieses Dienstes können Sie ein System auch vollständig ohne lokale Festplatte betreiben. Für diesen Fall empfiehlt es sich, das `root`-Filesystem per NFS zur Verfügung zu stellen.

4.3.1 Konfiguration des tftpd

Der eigentliche Bootvorgang ist zweistufig. Das erste Bootimage, das vom Rechner geladen wird, unterscheidet sich je nach Architektur.

► **x86**
Das PXE Image `pxelinux.0` wird vom BIOS geladen. Dieses übernimmt die Kontrolle über den weiteren Bootvorgang. PXE holt sich zunächst vom tftp Server eine Konfigurationsdatei. ◄

► **IPF**
Die Firmware des Rechners lädt zunächst vom tftp Server das Bootimage `elilo.efi`. Dieses lädt danach ebenfalls vom tftp Server eine Konfigurationsdatei, die den weiteren Bootvorgang steuert. ◄

► **POWER**
Hinweise zur Konfiguration sind dem folgenden Dokument zu entnehmen:
`http://penguinppc.org/~hollis/linux/rs6k-netboot.shtml`
◄

Legen Sie zunächst das Hauptverzeichnis für den tftpd an. Dies ist per Definition das Verzeichnis `/tftpboot/`:

```
mkdir /tftpboot
```

tftp für PXE boot vorbereiten

Das Bootimage, das zum Betrieb von PXE benötigt wird, finden Sie im Paket `syslinux` unter `/usr/share/syslinux/pxelinux.0`. Kopieren Sie diese Datei in das Verzeichnis `/tftpboot/`:

```
cp /usr/share/syslinux/pxelinux.0 /tftpboot
```

Die Konfigurationsdatei für PXE wird im Verzeichnis `/tftpboot/pxelinux.cfg/` abgelegt. Hierbei kann man eine Standardkonfigurationsdatei für alle Rechner anlegen, die gebootet werden sollen, es ist aber auch möglich, für jede IP-Adresse eine eigene Konfigurationsdatei zu verwenden. Wenn Sie zum Beispiel für die IP-Adresse 192.168.0.0 eine eigene Konfigurationsdatei erstellen möchten, so finden Sie deren Name mit dem Befehl `gethostip 192.168.0.0` heraus. Wenn keine spezielle Konfigurationsdatei gefunden wird, dann versucht PXE zuletzt eine Datei mit Namen `default` zu öffnen.

In der Konfigurationsdatei zu PXE stehen Ihnen einige Optionen zur Verfügung. Typischerweise sieht eine Konfigurationsdatei zur Installation eines Rechners folgendermaßen aus:

```
default linux
label linux
  kernel linux
  append initrd=initrd ramdisk_size=65536 install=slp:

implicit        0
display         message
prompt          1
timeout         200
notice          2
```

Damit diese Konfiguration funktioniert, müssen Sie noch die Dateien `linux` und `initrd` von der ersten Installations CD in das Verzeichnis `/tftpboot/` kopieren. Auf der CD finden Sie diese Dateien unter `/boot/loader/`. Weiterhin müssen Sie eine Installationsquelle einrichten, die per SLP verfügbar ist. Die Vorgehensweise hierzu wird in Abschnitt 4.1 auf Seite 166 beschrieben.

tftp zum Boot von Itanium Processor Family Rechnern vorbereiten

Das Image, das zum Netzwerkboot von Itanium Processor Family Rechnern benötigt wird, ist auf der ersten CD von SUSE LINUX Enterprise

Server in der Datei `/boot/image` enthalten. Zur Vorbereitung des Bootvorgangs ist es nötig, die Datei `bootia64.efi` aus diesem Image zu extrahieren, und als `elilo.efi` in das Verzeichnis `/tftpboot/` zu kopieren. Zum Start des Bootvorgangs müssen ausserdem die Dateien `linux`, `initrd`, `textmenu` und `elilo.conf` nach `/tftpboot/` kopiert werden. Unter der Annahme, dass die erste CD im Verzeichnis `/media/cdrom/` verfügbar ist, können Sie dies mit Hilfe folgender Befehle erreichen:

```
mount -o loop,ro /media/cdrom/boot/image /mnt
cd /mnt/efi/boot
cp -p linux initrd textmenu elilo.conf /tftpboot
cp -p bootia64.efi /tftpboot/elilo.efi
umount /mnt
```

Als letzten Schritt müssen Sie nun noch in der Datei `/tftpboot/elilo.conf` die `append` Zeilen durch einen weiteren Parameter `install=slp:` ergänzen. Dadurch wird dem Installationssystem gesagt, dass es seine Installationsquelle über das „SLP“ Protokoll suchen soll.

4.3.2 Einrichten des dhcpd

Der dhcpd übernimmt die Aufgabe, dem Rechner mitzuteilen, wo er das Bootimage findet. Weiterhin bekommt der Rechner, der ja als Netzwerkclient fungiert, eine IP-Adresse zugewiesen. Zur Konfiguration des dhcpd steht Ihnen ein YaST-Modul zur Verfügung. Einem Client teilen Sie den Ort des Bootimages mit Hilfe des Parameters `filename` mit.

► **x86, AMD64, EM64T**

```
filename "pxelinux.0";
```

◄

► **IPF**

```
filename "elilo.efi";
```

◄

Wenn der tftpd nicht auf dem selben Server wie der dhcpd läuft, müssen Sie die Adresse des tftpd-Servers ebenfalls in die Konfiguration eintragen:

```
next-server sun
```

4.3.3 Start des Bootvorgangs

Beim Bootvorgang such das BIOS des Rechners automatisch nach einer Bootquelle. Der dhcp Server antwortet auf diese Anfrage, und übermittelt die nötigen Daten, um per PXE oder elilo zu booten.

Vor dem eigentlichen Bootvorgang wird Ihnen ein „boot:“ Prompt angezeigt, an dem Sie bei Bedarf zusätzliche Parameter für Kernel und linuxrc übergeben können.

Update des Systems und Paketverwaltung

SUSE LINUX bietet die Möglichkeit, ein bestehendes System ohne Neuinstallation zu aktualisieren. Dabei muss unterschieden werden zwischen der *Aktualisierung einzelner Softwarepakete* und einem *Update des gesamten Systems*.

Einzelne Pakete können auch von Hand mit dem Paketmanager rpm installiert werden.

5.1 SUSE LINUX aktualisieren 178
5.2 Softwareänderungen von Version zu Version . . . 183
5.3 RPM – Der Paket-Manager der Distribution 190

5.1 SUSE LINUX aktualisieren

Es ist ein bekanntes Phänomen, dass Software von Version zu Version wächst. Deshalb empfiehlt es sich *vor* dem Update mit `df` nachzuschauen, wie sehr die einzelnen Partitionen bereits ausgelastet sind. Wenn Sie den Eindruck haben, es könnte knapp werden, dann führen Sie bitte vor dem Update ein Datenbackup durch und partitionieren Sie das System neu. Es kann kein genereller Tipp gegeben werden, wie viel Platz jeweils im Einzelnen benötigt wird – der Platzbedarf ist abhängig von der Art der bestehenden Partitionierung, von der ausgewählten Software und von der Versionsnummer des bestehenden Systems auf die aktuelle SUSE LINUX Distribution.

Hinweis

Es ist empfehlenswert, auf der CD die Datei `LIESMICH` bzw. `README` zu lesen; dort notieren wir zusätzliche Änderungen, die *nach* der Drucklegung des Handbuchs erfolgt sind.

Hinweis

5.1.1 Vorbereitungen

Vor Beginn eines Updates sollten sicherheitshalber die alten Konfigurationsdateien auf ein separates Medium (Streamer, Wechselplatte, ZIP-Laufwerk, CD-ROM etc.) kopiert werden. In erster Linie handelt es sich um die Dateien, die in `/etc` gespeichert sind; weiterhin sind z. T. die Verzeichnisse und Dateien unter `/var` sowie unter `/opt` zu kontrollieren und ggf. zu sichern. Zudem kann es nichts schaden, die aktuellen Benutzerdaten unter `/home` (die `HOME`-Verzeichnisse) auf ein Backup-Medium zu schreiben. Das Sichern der Daten ist als Systemadministrator `root` durchzuführen; nur `root` hat die Rechte, alle lokalen Dateien zu lesen. Bevor Sie den Update-Vorgang einleiten, notieren Sie sich die Rootpartition; mit dem Kommando `df /` können Sie den Gerätenamen der Rootpartition herausfinden; in dem Fall der Ausgabe 5.1 ist `/dev/hda2` die zu notierende Root-Partition.

***Beispiel 5.1:** Überblick mit df -h*

```
Dateisystem Größe Benut Verf  Ben% montiert auf
/dev/hda1   1,9G  189M  1.7G  10%  /dos
/dev/hda2   8,9G  7,1G  1,4G  84%  /
/dev/hda5   9,5G  8,3G  829M  92%  /home
```

Die Ausgabe zeigt, dass die Partition `/dev/hda2` unter `/` in das Dateisystem eingehängt (gemountet) ist.

5.1.2 Mögliche Probleme

passwd und group in /etc überprüfen

Vor dem Update muß sichergestellt werden, daß `/etc/passwd` und `/etc/group` keine Syntaxfehler enthalten. Rufen Sie zu diesem Zweck als `root` die Prüfprogramme `pwck` und `grpck` auf und beseitigen Sie Fehler, die gemeldet werden.

PostgreSQL

Vor einem PostgreSQL-Update (`postgres`) empfiehlt es sich in der Regel, die Datenbanken zu dumpen; vgl. die Manualpage von `pg_dump`. Dies ist natürlich nur dann erforderlich, wenn Sie PostgreSQL vor dem Update tatsächlich *benutzt* haben.

x86: Promise-Controller

Die Festplatten-Controller der Firma Promise finden sich inzwischen auf hochwertigen Mainboards in verschiedenen Rechnern. Manchmal als reine IDE-Controller (für UDMA 100), manchmal als IDE-RAID-Controller. Seit SUSE LINUX 8.0 werden diese Controller direkt vom Kernel unterstützt und als normale Controller für IDE-Festplatten behandelt. Erst das zusätzlich Kernel-Modul `pdcraid` ermöglicht die RAID-Funktionalität.

In manchen Fällen kann es beim Update passieren, dass Festplatten am Promise-Controller vor den Festplatten am normalen IDE-Controller erkannt werden. Das System wird dann nach einem Kernel-Update nicht mehr booten und sich typischerweise mit `Kernel panic: VFS: unable to mount root fs` verabschieden. In diesem Fall muss beim Booten der Kernel-Parameter `ide=reverse` angegeben werden, um die Reihenfolge der Plattenerkennung umzudrehen; vgl. Abschnitt 3.3 auf Seite 137 . Dieser Parameter muss für dauerhafte Verwendung mit YaST in die Bootkonfiguration eingetragen werden.

Achtung

Nur die im BIOS eingeschalteten Controller werden gefunden. Insbesondere hat das nachträgliche Ein- oder Ausschalten von Controllern im BIOS direkte Auswirkungen auf die Devicenamen. Bei unbedachtem Vorgehen ist unter Umständen das Booten nicht mehr möglich!

Achtung

Technische Erklärung Die Reihenfolge der Controller hängt vom Mainboard ab, jeder Hersteller hat seine eigene Strategie, Zusatzcontroller zu verdrahten. Mit dem Befehl `lspci` wird diese Reihenfolge sichtbar. Wenn der Promise-Controller vor dem normalen IDE-Controller aufgeführt wird, ist der Kernel-Parameter `ide=reverse` nach einem Update notwendig. Mit dem alten Kernel (ohne direkte Promise Unterstützung) wurde der Controller ignoriert und der normale IDE-Controller zuerst erkannt. Die erste Platte war dann `/dev/hda`. Mit dem neuen Kernel wird der Promise-Controller direkt gefunden und seine (bis zu vier) Platten als `/dev/hda`, `/dev/hdb`, `/dev/hdc` und `/dev/hdd` gemeldet. Die bisherige `/dev/hda`-Platte wird plötzlich zu `/dev/hde` und daher beim Bootvorgang nicht mehr gefunden.

5.1.3 Update mit YaST

Nach den in Abschnitt 5.1.1 auf Seite 178 genannten Vorarbeiten leiten Sie den Bootvorgang ein.

1. Starten Sie das System wie zur Installation und wählen Sie dann in YaST — nach Festlegung der Sprache — *nicht* 'Neuinstallation', sondern 'Update des bestehenden Systems'.

2. YaST wird ermitteln, ob mehr als eine Rootpartition vorhanden ist; falls nein, geht es weiter mit dem Systembackup. Falls mehrere Partitionen vorhanden sind, müssen Sie die richtige Partition auswählen und mit 'Weiter' bestätigen (beim Beispiel in Abschnitt 5.1.1 auf Seite 178 hatten Sie `/dev/hda2` notiert).

   YaST wird alte `fstab` einlesen, die sich auf dieser Partition befindet, um dann die dort eingetragenen Dateisysteme zu analysieren und schließlich zu mounten.

3. Danach besteht die Möglichkeit, eine Sicherungskopie der Systemdateien während des Updates erstellen zu lassen. Diese Option verlangsamt den Update-Vorgang, sollte aber gewählt werden, wenn Sie kein aktuelles Systembackup haben.

4. Entweder kann im folgenden Dialog festgelegt werden, dass nur die bereits installierte Software erneuert wird oder dass dem System wichtige neue Softwarekomponenten hinzugesellt werden (Upgrade-Modus). Es ist empfehlenswert, die vorgegebene Zusammenstellung zu akzeptieren (zum Beispiel 'Standard-System'). Etwaige Unstimmigkeiten können Sie mit YaST später beseitigen.

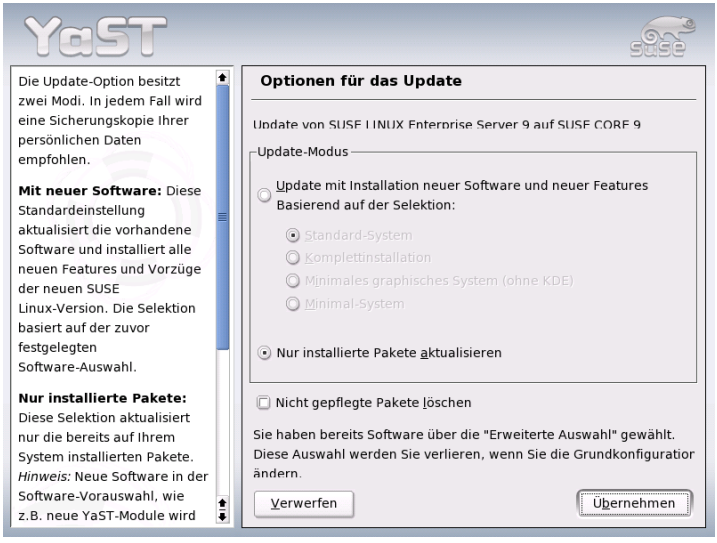

Abbildung 5.1: *Update der Software*

5.1.4 Manuell gesteuertes Update

Das Basissystem erneuern

Da beim Aktualisieren des Grundsystems die zentralen Bestandteile des Systems (wie zum Beispiel Bibliotheken) ausgetauscht werden müssen, kann diese Aufgabe nicht im normalen Betrieb, das heisst aus dem bereits laufenden Linuxsystem heraus, erledigt werden.

Sie müssen also die Update-Umgebung starten. Dies geschieht im Normalfall mit der CD bzw. DVD oder mit der selbst erstellten Diskette zum Booten (Bootdisk). Wenn Sie manuelle Eingriffe während des Updates vornehmen oder das gesamte Update mit der ncurses-ui von YaST (Textmodus) durchführen wollen, sind im Wesentlichen die Schritte notwendig, die bereits in Abschnitt 3.3 auf Seite 137 ff. ausführlich beschrieben sind:

1. Direkt im Anschluss an das Booten des Kernels von der Bootdisk oder der CD bzw. DVD wird automatisch linuxrc gestartet.
2. Im linuxrc sind im Hauptmenü unter dem Menüpunkt 'Einstellungen' Sprache und Tastatur festzulegen und jeweils mit 'Ok' zu bestätigen.
3. Über den Menüpunkt 'Kernel-Module' müssen ggf. die notwendigen Hardware- und Software-Treiber geladen werden; zum genauen Vorgehen vgl. Abschnitt 3.1.1 auf Seite 126 und die linuxrc-Beschreibung 3.1.4 auf Seite 128.
4. Es kann über die Menüpunkte 'Installation / System starten' -> 'Installation/Update starten' zur Auswahl des Quellmediums übergegangen werden (vgl. Abschnitt 3.1.6 auf Seite 131).
5. Von linuxrc wird die Installationsumgebung geladen und es wird YaST gestartet.

Im Eingangsmenü von YaST wählen Sie — nach Kontrolle der Sprache und Überprüfung der Hardware durch YaST — den Punkt 'Update des bestehenden Systems'.

Im Anschluss versucht YaST, die Root-Partition herauszufinden und bietet das Ergebnis zur Auswahl bzw. Bestätigung an; in der angezeigten Liste geben Sie Ihre Root-Partition an, wie oben notiert (Beispiel: `/dev/hda2`). So beauftragen Sie YaST, die alte `fstab` einzulesen, die sich auf dieser Partition befindet; YaST wird die dort eingetragenen Dateisysteme analysieren und dann mounten.

Danach besteht die Möglichkeit, eine Sicherungskopie der Systemdateien während des Updates erstellen zu lassen.

Entweder kann im folgenden Dialog festgelegt werden, dass nur die bereits installierte Software erneuert wird oder dass dem System wichtige neue Softwarekomponenten hinzugesellt werden (Upgrade-Modus). Es ist empfehlenswert, die vorgegebene Zusammenstellung zu akzeptieren (zum Beispiel 'Standard-System'). Etwaige Unstimmigkeiten können Sie mit YaST beseitigen.

Warndialog: 'Ja', damit das Übertragen der neuen Software von dem Quellmedium auf die Festplatte des Systems geschehen kann. Es folgt die Überprüfung der RPM-Datenbank.

Anschließend werden zunächst die zentralen Bestandteile des Systems aktualisiert, wobei YaST automatisch Sicherungen von Dateien anlegt, die seit der letzten Installation während des Betriebs verändert wurden; weiterhin werden alte Konfigurationsdateien ggf. mit der Endung `.rpmorig` bzw. `.rpmsave` gesichert; der Vorgang der Installation bzw. des Updates wird in `/var/log/YaST2/y2log*` protokolliert und ist jederzeit nachlesbar.

Update des restlichen Systems

Ist das Basissystem aktualisiert, gelangen Sie in einen speziellen Update-Modus von YaST. Dort können Sie nach Ihren Wünschen den Rest des Systems updaten.

Nachdem diese Aufgabe erledigt ist, müssen Sie den Vorgang wie eine Erstinstallation abschließen. Unter anderem sollten Sie einen neuen Kernel auswählen; YaST wird diese Option anbieten.

Mögliche Probleme

Falls sich nach dem Update bestimmte Shell-Umgebungen nicht mehr so verhalten wie gewohnt, kontrollieren Sie bitte unbedingt, ob die aktuellen Punkt-Dateien im Homeverzeichnis noch zum System passen. Ist dies nicht der Fall, übernehmen Sie bitte die aktuellen Versionen von `/etc/skel`; zum Beispiel: `cp /etc/skel/.profile  /.profile`.

5.2 Softwareänderungen von Version zu Version

In den folgenden Abschnitten wird aufgelistet, welche Details sich von Version zu Version geändert haben. In dieser Übersicht erscheint beispielsweise, ob grundlegende Einstellungen neu vorgenommen oder ob Konfigurationsdateien an andere Stellen verschoben wurden oder ob bekannte Programme erkennbar modifiziert wurden. Es werden die Dinge genannt, die den Benutzer bzw. den Administrator bei der täglichen Arbeit unmittelbar berühren.

5.2.1 Von SLES8 auf SLES9

Umstellung auf Kernel 2.6

SUSE LINUX wurde komplett auf die Kernelversion 2.6 umgestellt; die Vorgängerversion 2.4 sollte nicht mehr verwendet werden, da die mitgelieferten Programme mit Kernel 2.4 möglicherweise nicht funktionieren. Weiterhin sind folgende Einzelheiten zu beachten:

- Das Laden der Module werden nun über die Datei `/etc/modprobe.conf` konfiguriert; die Datei `/etc/modules.conf` ist obsolet. YaST wird die Datei versuchen zu konvertieren (vgl. auch das Skript `/sbin/generate-modprobe.conf`).
- Module haben nun das Suffix `.ko`.
- Das Modul `ide-scsi` wird beim Brennen von CDs nicht mehr benötigt.
- Bei den Optionen der ALSA-Soundmodule ist das Prefix `snd_` entfernt worden.
- `sysfs` ergänzt nun `/proc`-Dateisystem.
- Das Powermanagement (speziell ACPI) wurde verbessert und kann nun über ein YaST-Modul eingestellt werden.

Codepage und Einhängen von VFAT-Partitionen

Beim Mounten von VFAT-Partitionen muss der Parameter `code=` in `codepage=` geändert werden. Falls das Mounten einer VFAT-Partition Probleme bereitet, prüfen Sie, ob die Datei `/etc/fstab` den alten Parameternamen enthält.

Eingabegeräte (Input Devices)

Zu den Änderungen bei den Eingabegeräten (*Input Devices*) vgl. den oben genannten Portalartikel (`http://portal.suse.de/sdb/de/2004/02/bugs91.html`).

Native POSIX Thread Library und glibc 2.3.x

Programme, die gegen NGPT (*Next Generation POSIX Threading*) gelinkt sind, laufen nicht mit glibc 2.3.x. Alle davon betroffenen Programme, die nicht mit SUSE LINUX mitgeliefert werden, müssen entweder mit linuxthreads oder NPTL (*Native POSIX Thread Library*) neu kompiliert werden. Bei der Portierung ist NPTL zu bevorzugen, da das der in die Zukunft weisende Standard ist.

Bei Schwierigkeiten mit NPTL kann auf die älteren linuxthreads-Implementierung durch das Setzen der folgenden Umgebungsvariablen ausgewichen werden (dabei muss ⟨*kernel-version*⟩ durch die Versionsnummer des entsprechenden Kernels ersetzt werden):

```
LD_ASSUME_KERNEL=kernel-version
```

Dabei sind folgende Versionsnummern möglich:

2.2.5 (i386, i586): linuxthreads ohne Floating Stacks

2.4.1 (AMD64, IPF, s390x, i586, i686):
linuxthread mit Floating Stacks

Hinweise zum Kernel und linuxthreads *mit* Floating Stacks:

Programme, die `errno`, `h_errno` und `_res` verwenden, müssen die einschlägigen Header-Dateien (`errno.h`, `netdb.h` und `resolv.h`) mit `#include` einbinden. C++-Programme mit Multithread-Unterstützung, die *Thread Cancellation* verwenden, müssen mit der Umgebungsvariablen `LD_ASSUME_KERNEL=2.4.1` dazu gebracht werden, die Bibliothek linuxthreads zu verwenden.

Anpassungen für Native POSIX Thread Library

NPTL (*Native POSIX Thread Library*) ist als Thread-Paket dabei. NPTL wurde binärkompatibel zu der älteren Bibliothek linuxthreads entwickelt. An den Stellen jedoch, an denen linuxthreads gegen den POSIX-Standard verstößt, erfordert NPTL Anpassungen; im Einzelnen sind zu nennen: Signal-Behandlung; `getpid` liefert in allen Threads denselben Wert zurück; Threads-Handlers, die mit pthread_atfork registriert sind, laufen nicht, wenn `vfork` verwendet wird.

Konfiguration der Netzwerkschnittstelle

Die Konfiguration der Netzwerkschnittstelle hat sich geändert. Bisher wurde nach der Konfiguration einer nicht vorhandenen Schnittstelle die Initialisierung der Hardware gestartet. Nun wird nach neuer Hardware gesucht und diese sogleich initialisiert, woraufhin die neue Netzwerkschnittstelle konfiguriert werden kann.

Zusätzlich wurden für die Konfigurationsdateien neue Namen eingeführt. Da der Name einer Netzwerkschnittstelle dynamisch erzeugt wird und der Einsatz von Hotplug-Geräten beständig zunimmt, ist ein Name wie `eth`⟨*X*⟩ nicht mehr für Konfigurationszwecke geeignet. Deshalb verwenden wir nun eindeutige Beschreibungen wie die MAC-Adresse oder den PCI-Slot für die Benennung der Schnittstellenkonfigurationen.

Hinweis: Sie können Schnittstellennamen natürlich verwenden, sobald Sie erscheinen. Befehle wie `ifup eth0` bzw. `ifdown eth0` sind immer noch möglich.

Die Gerätekonfigurationen finden Sie in `/etc/sysconfig/hardware`. Die von diesen Geräten bereitgestellten Schnittstellen finden sich üblicherweise (nur mit unterschiedlichen Namen) in `/etc/sysconfig/network`.

Vgl. die detaillierte Beschreibung unter `/usr/share/doc/packages/sysconfig/README`.

Top-Level-Domain .local als link-local-Domain

Die Resolver-Bibliothek behandelt die Top-Level-Domain `.local` als „link-local“-Domain und sendet Multicast-DNS-Anfragen an die Multicast-Adresse `224.0.0.251` Port `5353` anstelle normaler DNS-Anfragen; dies ist eine inkompatible Änderung. Falls bereits die Domain `.local` in der Nameserver-Konfiguration verwendet wird, muss auf einen anderer Domainnamen ausgewichen werden. Weitere Informationen zu Multicast-DNS finden Sie unter `http://www.multicastdns.org`.

UTF-8 als systemweite Kodierung

Als Kodierung für das System ist nun `UTF-8` voreingestellt. Bei einer Standardinstallation wird also eine Locale mit `.UTF-8` als Kodierungsangabe (*Encoding*) festgelegt (z.B. `de_DE.UTF-8`). Mehr Informationen unter `http://www.suse.de/~mfabian/suse-cjk/locales.html`.

Dateinamen nach UTF-8 konvertieren

Dateien in Dateisystemen, die früher erstellt wurden, verwenden (sofern nicht anders angegeben) keine UTF-8-Kodierung für die Dateinamen. Sollten diese Dateien andere als ASCII-Zeichen enthalten, werden sie nun „zerstümmelt“ angezeigt. Zur Berichtigung kann das Skript `convmv` verwendet werden, welches die Kodierung der Dateinamen nach UTF-8 umwandelt.

Shell-Tools kapatibel mit POSIX-Standard von 2001

Shell-Tools aus dem `coreutils` wie `tail`, `chown`, `head`, `sort` etc. folgen in der Vorgabeeinstellung nun dem POSIX-Standard von 2001 (*Single UNIX Specification, version 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*) und nicht mehr dem Standard von 1992. Das alte Verhalten kann man mit einer Umgebungsvariablen erzwingen:

```
_POSIX2_VERSION=199209
```

Der neue Wert ist 200112 und wird als Vorgabe für `_POSIX2_VERSION` angenommen. Den SUS-Standard kann man hier nachlesen (frei, aber eine Registrierung ist erforderlich):

`http://www.unix.org`

Hier eine kurze Gegenüberstellung:

Tabelle 5.1: *Gegenüberstellung POSIX 1992/POSIX 2001*

POSIX 1992	POSIX 2001
chown tux.users	chown tux:users
tail +3	tail -n +3
head -1	head -n 1
sort +3	sort -k +3
nice -10	nice -n 10
split -10	split -l 10

Hinweis

Software von Drittanbietern folgt möglicherweise noch nicht dem neuen Standard; in einem solchen Fall ist es ratsam, die Umgebungsvariable wie oben beschrieben zu setzen: `_POSIX2_VERSION=199209`.

Hinweis

/etc/gshadow obsolet

`/etc/gshadow` wurde aufgegeben und entfernt, da die Datei überflüssig ist; die Gründe dafür sind:

- Seitens der glibc gibt es keine Unterstützung.
- Es gibt keine offizielle Schnittstelle für diese Datei; sogar in der shadow-Suite gibt es keine solche Schnittstelle.
- Die meisten Tools, die das Gruppenpasswort überprüfen, unterstützen die Datei nicht und ignorieren sie aus den eben genannten beiden Gründen.

OpenLDAP

- Da sich das Datenbankformat geändert hat, müssen die Datenbanken neu erstellt werden. Beim Update wird versucht, diese Konvertierung automatisch durchzuführen; es wird aber bestimmt Fälle geben, in denen die Konvertierung scheitert.
- Die Schema-Überprüfung wurde wesentlich verbessert. Dadurch werde einige (nicht standardkonforme) Operationen, die mit dem frühren LDAP-Server möglich waren, nun nicht mehr möglich sein.
- Die Syntax der config-Datei hat sich teilweise in Hinblick auf ACLs geändert.

Weitere Informationen zum Update finden Sie nach der Installation in der Datei `/usr/share/doc/packages/openldap2/README.update`

Apache 1.3 durch Apache 2 ersetzt

Der Apache Webserver (Version 1.3) wurde ersetzt durch Apache 2. Ein Update von auf einem System mit einer Installation eines HTTP-Servers wird das Apache Paket löschen und Apache 2 installieren. Das System muss dann durch YaST oder manuell angepasst werden. Konfigurationsdateien unter `/etc/httpd` sind nun in `/etc/apache2`. Apache 2 benötigt eines der Pakete `apache2-prefork` (empfohlen für Stabilität) oder `apache2-worker` Paket.

Von samba 2.x auf samba 3.x

Mit dem Update von samba 2.x auf samba 3.x steht die `winbind`-Authentifikation nicht mehr zur Verfügung; die anderen Methoden sind weiterhin möglich. Aus diesem Grund wurden die folgenden Programme entfernt:

```
/usr/sbin/wb_auth
/usr/sbin/wb_ntlmauth
/usr/sbin/wb_info_group.pl
```

Vgl. auch: `http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5`

OpenSSH-Update (Version 3.8p1)

Die `gssapi`-Unterstützung wurde durch `gssapi-with-mic` ersetzt, um mögliche MITM-Angriffe zu beheben. Diese beiden Versionen sind nicht kompatibel. Das bedeutet, dass Sie sich nicht von älteren Distributionen mit Kerberos-Tickets authentifizieren können, da andere Methoden zur Authentifikation verwendet werden.

SSH- und Terminal-Applikationen

Bei Zugriff von einem entfernten Rechner (vor allem SSH, telnet und RSH) zwischen der Version 9 (in der Standardkonfiguration mit aktiviertem UTF-8) und älteren Systemen (SLES, SLES 8 oder SUSE LINUX 9.0 und früher, wobei UTF-8 nicht standardmäßig aktiviert oder unterstützt ist), können Terminal-Applikationen fehlerhafte Zeichen ausgeben.

Dies liegt daran, dass OpenSSH keine lokalen Einstellungen weiterleitet, sodass System-Standardeinstellungen verwendet werden, die möglicherweise nicht mit den entfernten Terminal-Einstellungen übereinstimmen.

Dies betrifft YaST im Textmodus sowie Applikationen, die von einem entfernten Rechner als normaler Benutzer (nicht `root`) ausgeführt werden. Die von `root` ausgeführten Applikationen sind nur dann betroffen, wenn der Benutzer die Standard-Locales für `root` ändert (nur `LC_CTYPE` wird standardmäßig gesetzt).

libiodbc wurde verworfen

Anwender von FreeRADIUS müssen nun gegen unixODBC linken, da libiodbc verworfen wurde.

XML-Ressourcen in /usr/share/xml

Der FHS (siehe 10.1.2 auf Seite 268) sieht nun vor, dass XML-Ressourcen (DTDs, Stylesheets etc.) unter `/usr/share/xml` installiert werden. Aus diesem Grund sind einige Verzeichnisse nun nicht mehr unter `/usr/share/sgml` zu finden. Bei Problemen müssen entweder die eigenen Skripte oder Makefiles angepaßt bzw. die offiziellen Kataloge (insbesondere `/etc/xml/catalog` bzw. `/etc/sgml/catalog`) verwendet werden.

Wechselmedien mit subfs

Wechselmedien werden nun über subfs integriert. Die Medien müssen nun nicht mehr manuell eingehangen (`mount`) werden. Der Befehl `cd /media/*` startet das automatische Einhängen. Medien können nicht ausgeworfen werden, solange ein Programm darauf zugreift.

Druckerkonfiguration

Informationen zu den Änderungen am Drucksystem finden Sie in dem Abschnitt 13.1 auf Seite 324 .

5.3 RPM – Der Paket-Manager der Distribution

Bei SUSE LINUX kommt RPM (engl. *RPM Package Manager*) mit den Hauptprogrammen `rpm` und `rpmbuild` als Management für die Softwarepakete zum Einsatz. Damit steht den Benutzern, den Systemadministratoren und nicht zuletzt dem Pakete-Macher die mächtige RPM-Datenbank

zur Verfügung, über die jederzeit detaillierte Informationen zur installierten Software abgefragt werden können.

Im Wesentlichen kann `rpm` in fünf Modi agieren: Softwarepakete installieren bzw. de-installieren oder updaten, die RPM-Datenbank neu erstellen, Anfragen an die RPM-Datenbank bzw. an einzelne RPM-Archive richten, Pakete auf Integrität überprüfen und Pakete signieren. `rpmbuild` dient dazu, installierbare Pakete aus den unangetasteten Quellen (engl. *pristine sources*) herzustellen.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt; die Archive bestehen aus den zu installierenden (Programm-)Dateien und aus verschiedenen Meta-Informationen, die während der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank abgelegt werden. RPM-Archive haben die Dateinamen-Endung `.rpm`.

Mit `rpm` lassen sich LSB-konforme Pakete verwalten; zu LSB vgl. Abschnitt 10.1.1 auf Seite 268.

Hinweis

Bei etlichen Paketen sind die für die Software-Entwicklung notwendigen Komponenten (Bibliotheken, Header- und Include-Dateien etc.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software *selbst* übersetzen (kompilieren) wollen – beispielsweise neuere GNOME-Pakete . Solche Pakete sind in der Regel an dem Namenszusatz `-devel` zu erkennen: `alsa-devel`, `gimp-devel`, `kdelibs-devel` etc.

Hinweis

5.3.1 Prüfen der Authentizität eines Pakets

RPM-Pakete von SUSE LINUX sind mit GnuPG signiert:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

Mit folgenem Befehl kann man die Signatur eines RPM-Pakets überprüfen und so feststellen, ob es wirklich von SUSE oder einer anderen vertrauenswürdigen Stelle stammt:

```
rpm --checksig apache-1.3.12.rpm
```

Insbesondere bei Updatepaketen aus dem Internet ist diese Vorsichtsmaßname zu empfehlen. Unser öffentlicher Paketsignierschlüssel ist standardmäßig in `/root/.gnupg/` hinterlegt. Seit Version 8.1 liegt der Schlüssel zusätzlich im Verzeichnis `/usr/lib/rpm/gnupg/`, damit auch normale Benutzer die Signatur von RPM-Paketen prüfen können.

5.3.2 Pakete verwalten: Installieren, Updaten und Deinstallieren

Im Normalfall ist das Installieren eines RPM-Archivs schnell erledigt:

```
rpm -i <paket>.rpm
```

Mit diesem Standardbefehl wird ein Paket aber nur dann installiert, wenn die Abhängigkeiten erfüllt sind und wenn es zu keinen Konflikten kommen kann; `rpm` fordert per Fehlermeldung die Pakete an, die zum Erfüllen der Abhängigkeiten notwendig sind. Die Datenbank wacht im Hintergrund darüber, dass es zu keinen Konflikten kommt: Eine Datei darf in der Regel nur zu einem Paket gehören. Mit verschiedenen Optionen kann man sich über diese Regel hinwegsetzen. Wer dies tut, der sollte aber genau wissen, was er tut, da er damit eventuell die Updatefähigkeit des Systems aufs Spiel setzt.

Interessant sind auch die Optionen `-U` bzw. `--upgrade` und `-F` bzw. `--freshen`, um ein Paket zu aktualisieren.

```
rpm -F <paket>.rpm
```

Dadurch wird eine ältere Version des gleichen Pakets gelöscht und die neue Version installiert. Der Unterschied zwischen den beiden Versionen liegt darin, dass bei `-U` auch Pakete installiert werden, die bisher nicht im System verfügbar waren, während die Option `-F` nur dann ein Paket erneuert, wenn es bereits zuvor installiert war. Gleichzeitig versucht `rpm`, sorgfältig mit den *Konfigurationsdateien* umzugehen, wobei – etwas vereinfacht – die folgende Strategie zum Tragen kommt:

- Falls eine Konfigurationsdatei vom Systemadministrator nicht verändert wurde, wird von `rpm` die neue Version der entsprechenden Datei installiert. Es sind keine Eingriffe seitens des Administrators notwendig.

- Falls eine Konfigurationsdatei vom Administrator zu irgendeinem Zeitpunkt vor dem Update geändert wurde, wird `rpm` die geänderte Datei dann – und nur dann – mit der Erweiterung `.rpmorig` oder `.rpmsave` sichern und die neue Version aus dem RPM-Paket installieren, falls sich zwischen ursprünglicher Datei und der Datei aus dem Update-Paket etwas geändert hat. In diesem Fall ist es sehr wahrscheinlich, dass Sie die frisch installierte Konfigurationsdatei anhand der Kopie (`.rpmorig` oder `.rpmsave`) auf Ihre Systembedingungen hin abstimmen müssen.
- `.rpmnew`-Dateien werden immer dann auftauchen, wenn es die Konfigurationsdatei bereits gibt *und* wenn in der `.spec`-Datei die `noreplace`-Kennung gesetzt wurde.

Im Anschluss an ein Update sollten nach dem Abgleich alle `.rpmorig`-, `.rpmsave`- bzw. `.rpmnew`-Dateien entfernt werden, um bei folgenden Updates nicht zu stören. Die Erweiterung `.rpmorig` wird gewählt, wenn die Datei der RPM-Datenbank noch nicht bekannt war, sonst kommt `.rpmsave` zum Zuge; mit anderen Worten: `.rpmorig` entsteht beim Update von Fremdformat auf RPM und `.rpmsave` beim Update von RPM-alt auf RPM-neu. Bei `.rpmnew` kann keine Aussage gemacht werden, ob vom Systemadministrator eine Änderung an der Konfigurationsdatei vorgenommen wurde oder ob nicht. Eine Liste dieser Dateien finden Sie unter `/var/adm/rpmconfigcheck`.

Beachten Sie, dass einige Konfigurationsdateien (zum Beispiel `/etc/httpd/httpd.conf`) mit Absicht nicht überschrieben werden, um den sofortigen Weiterbetrieb mit den eigenen Einstellungen zu ermöglichen.

Die Option `-U` ist also mehr als ein Äquivalent für die Abfolge `-e` (Deinstallieren/Löschen) und `-i` (Installieren). Wann immer möglich, dann ist der Option `-U` der Vorzug zu geben.

Hinweis

Nach jedem Update müssen Sie die von `rpm` angelegten Sicherungskopien mit der Erweiterung `.rpmorig` oder `.rpmsave` kontrollieren, das sind Ihre alten Konfigurationsdateien. Falls erforderlich, übernehmen Sie bitte Ihre Anpassungen aus den Sicherungskopien in die neuen Konfigurationsdateien und löschen Sie dann die alten Dateien mit der Erweiterung `.rpmorig` bzw. `.rpmsave`.

Hinweis

YaST mit der Option `-i` ist in der Lage, alle Paketabhängigkeiten aufzulösen und eine entsprechende Installation durchzuführen:

```
yast -i <paket>
```

Wenn ein Paket entfernt werden soll, geht man ähnlich vor:

```
rpm -e <paket>
```

`rpm` wird ein Paket aber nur dann entfernen, wenn keine Abhängigkeiten mehr bestehen. So ist es zum Beispiel theoretisch nicht möglich, Tcl/Tk zu löschen, solange noch irgendein anderes Programm Tcl/Tk benötigt – auch darüber wacht RPM mithilfe der Datenbank. Falls in einem Ausnahmefall eine derartige Lösch-Operation nicht möglich sein sollte, obwohl keine Abhängigkeiten mehr bestehen, kann es hilfreich sein, die RPM-Datenbank mittels der Option `--rebuilddb` neu aufzubauen; vgl. unten die Anmerkungen zur RPM-Datenbank.

5.3.3 RPM und Patches

Um die Betriebssicherheit eines Systems zu gewährleisten, ist es notwendig, von Zeit zu Zeit Pakete in das System einzuspielen, die es auf einen neuen Stand bringen. Bisher konnte ein Fehler in einem Paket nur dadurch behoben werden, dass man das komplette Paket ersetzt hat. Bei großen Paketen mit kleinen Fehlern können so schnell große Datenmengen zusammen kommen. Seit der Version 8.1 gibt es bei SUSE daher ein neues Feature in RPM, das es ermöglicht, Patches zu Paketen einzuspielen.

Die interessantesten Informationen zu einem Patch-RPM sollen am Beispiel pine aufgezeigt werden:

- Passt das Patch-RPM zu meinem System?

  Um dies zu prüfen, sollten Sie zunächst die installierte Version des Paketes abfragen. Im Fall von pine geht das mit dem Befehl

  ```
  rpm -q pine
  pine-4.44-188
  ```

  Als Nächstes wird das Patch-RPM untersucht, ob es zu genau dieser Version von pine passt:

  ```
  rpm -qp --basedon pine-4.44-224.i586.patch.rpm
  pine = 4.44-188
  pine = 4.44-195
  pine = 4.44-207
  ```

Dieser Patch passt zu drei verschiedenen Versionen von pine. Auch die in unserem Fall installierte Version ist dabei enthalten, so dass der Patch eingespielt werden kann.

- Welche Dateien werden durch den Patch ersetzt?

  Die von einem Patch betroffenen Dateien können leicht aus dem Patch-RPM ausgelesen werden. Der Parameter `-P` von `rpm` dient dazu, spezielle patch-relevanten Möglichkeiten auszuwählen. Demnach bekommt man die Liste der Dateien mit

  ```
  rpm -qpPl pine-4.44-224.i586.patch.rpm
  /etc/pine.conf
  /etc/pine.conf.fixed
  /usr/bin/pine
  ```

  oder, wenn der Patch bereits installiert ist, mit

  ```
  rpm -qPl pine
  /etc/pine.conf
  /etc/pine.conf.fixed
  /usr/bin/pine
  ```

- Wie spielt man ein Patch-RPM in das System ein?

  Patch-RPMs werden wie normale RPMs verwendet. Der einzige Unterschied liegt darin, dass für sie ein passendes RPM bereits eingespielt sein muss.

- Welche Patches sind im System eingespielt und auf welchen Paketversionen haben sie aufgesetzt?

  Eine Liste aller Patches, die im System eingespielt sind bekommen Sie mit dem Befehl `rpm -qPa`. Wenn, wie in unserem Beispiel, in einem neuen System erst ein Patch eingespielt ist, sieht das so aus:

  ```
  rpm -qPa
  pine-4.44-224
  ```

  Wenn Sie nach einiger Zeit wissen möchten, welche Paketversion denn zunächst eingespielt war, so ist dies ebenfalls noch in der RPM-Datenbank vorhanden. Sie bekommen diese Information für `pine` mit dem Kommando:

  ```
  rpm -q --basedon pine
  pine = 4.44-188
  ```

Weitere Informationen, auch zum Patch-Feature von RPM, finden Sie in dem Manualpages von `rpm` und `rpmbuild`.

5.3.4 Anfragen stellen

Mit der Option `-q` (engl. *query*) leitet man Anfragen ein. Damit ist es möglich die RPM-Archive selbst zu durchleuchten (Option `-p` ⟨*PaketDatei*⟩) als auch die RPM-Datenbank zu befragen. Die Art der angezeigten Information kann man mit den zusätzlichen Optionen auswählen; vgl. Tabelle 5.2.

Tabelle 5.2: *Die wichtigsten Abfrageoptionen (-q [-p] paket)*

`-i`	Paket-Informationen anzeigen
`-l`	Dateiliste des Pakets anzeigen
`-f` ⟨*DATEI*⟩	Anfrage nach Paket, das die Datei ⟨*DATEI*⟩ besitzt; ⟨*DATEI*⟩ muss mit vollem Pfad angegeben werden!
`-s`	Status der Dateien anzeigen (impliziert `-l`)
`-d`	Nur Dokumentationsdateien auflisten (impliziert `-l`)
`-c`	Nur Konfigurationsdateien auf" | listen (impliziert `-l`)
`--dump`	Alle überprüfbaren Infos zu jeder Datei anzeigen (mit `-l`, `-c` oder `-d` benutzen!)
`--provides`	Fähigkeiten des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann
`--requires`, `-R`	Paket-Abhängigkeiten ausgeben
`--scripts`	Die diversen (De-)Installations-Skripten ausgeben

Der folgende Befehl gibt die Information in Ausgabe 5.2 aus:

```
rpm -q -i wget
```

Beispiel 5.2: *rpm -q -i wget*

```
Name        : wget                     Relocations: (not relocateable)
Version     : 1.8.2                    Vendor: SuSE Linux AG, Nuernberg, Germany
Release     : 301                      Build Date: Di 23 Sep 2003 20:26:38 CEST
Install date: Mi 08 Okt 2003 11:46:31 CEST      Build Host: levi.suse.de
Group: Productivity/Networking/Web/Utilities Source RPM: wget-1.8.2-301.src.rpm
Size        : 1333235                        License: GPL
Signature   : DSA/SHA1, Di 23 Sep 2003 22:13:12 CEST, Key ID a84edae89c800aca
Packager    : http://www.suse.de/feedback
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

Die Option `-f` führt nur dann zum Ziel, wenn man den kompletten Dateinamen, einschließlich des Pfades, kennt. Sie können beliebig viele zu suchende Dateinamen angeben, zum Beispiel:

```
rpm -q -f /bin/rpm /usr/bin/wget
```

führt zu dem Ergebnis:

```
rpm-3.0.3-3
wget-1.5.3-55
```

Kennt man nur einen Teil des Dateinamens, so muss man sich mit einem Shell-Skript behelfen (vgl. Datei 5.3); der gesuchte Dateiname ist als Parameter beim Aufruf des Skripts zu übergeben.

Beispiel 5.3: *Paket-Suchskript*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" ist in Paket:"
    rpm -q -f $i
    echo ""
done
```

Mit dem Befehl kann man sich gezielt die Auflistung der Informationen (Updates, Konfiguration, Änderungen etc.) zu einem bestimmten Paket anzeigen lassen; hier beispielsweise zu dem Paket `rpm`:

```
rpm -q --changelog rpm
```

Es werden allerdings nur die letzten 5 Einträge in der RPM-Datenbank angezeigt; im Paket selbst sind alle Einträge (der letzten 2 Jahre) enthalten. Diese Abfrage funktioniert, wenn CD 1 unter `/cdrom` eingehangen ist:

```
rpm -qp --changelog /cdrom/suse/i586/rpm-3*.rpm
```

Anhand der installierten Datenbank lassen sich auch Überprüfungen durchführen. Eingeleitet werden diese Vorgänge mit der Option `-V` (gleichbedeutend mit `-y` oder `--verify`). Damit veranlasst man `rpm`, all die Dateien anzuzeigen, die sich im Vergleich zur ursprünglichen Version, wie sie im Paket enthalten war, geändert haben. `rpm` stellt dem eigentlichen Dateinamen bis zu acht Zeichen voran, die auf folgende Änderungen hinweisen:

Tabelle 5.3: Die Überprüfungen

`5`	MD5-Prüfsumme
`S`	Dateigröße
`L`	Symbolischer Link
`T`	Modification Time
`D`	major und minor Gerätenummer (engl. *device number*)
`U`	Benutzer (engl. *user*)
`G`	Gruppe (engl. *group*)
`M`	Modus (einschl. Rechte und Typus)

Bei Konfigurationsdateien wird zusätzlich ein `c` ausgegeben. Beispiel, falls etwas an `/etc/wgetrc` aus dem `wget` geändert wurde:

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Die Dateien der RPM-Datenbank liegen unter `/var/lib/rpm/`.

Bei einer `/usr/`-Partition von 1 GB kann die Datenbank durchaus 30 MB Plattenplatz beanspruchen; insbesondere nach einem kompletten Update. Falls die Datenbank über Gebühr groß erscheint, ist es meist hilfreich, mit der Option `--rebuilddb` eine neue Datenbank auf Basis der existierenden zu erstellen. Es ist sinnvoll, vor einem solchen Rebuild eine Kopie der existierenden Datenbank aufzubewahren.

Weiterhin legt das `cron`-Skript `cron.daily` täglich gepackte Kopien der Datenbank unter `/var/adm/backup/rpmdb` an, deren Anzahl durch die Variable `MAX_RPMDB_BACKUPS` (Standard: `5`) in der `/etc/sysconfig/backup` vorgegeben wird; es ist mit bis zu 3 MB pro Backup bei einem 1 GB großen `/usr` Verzeichnis rechnen.

5.3.5 Quellpakete installieren und kompilieren

Alle Quellpakete haben die Erweiterung `.src.rpm` hinter dem eigentlichen Paketnamen; diese Dateien sind die „Source-RPMs“.

Hinweis

Diese Pakete können mit YaST – wie jedes andere Paket – installiert werden, allerdings werden Quellpakete nie als installiert (`[i]`) markiert wie die regulären anderen Pakete. Dies liegt daran, dass die Quellpakete nicht in die RPM-Datenbank aufgenommen werden; in der RPM-Datenbank nämlich erscheint nur *installierte* Betriebssoftware.

Hinweis

Die Arbeitsverzeichnisse für `rpm` bzw. `rpmbuild` unter `/usr/src/packages` müssen vorhanden sein (falls keine eigenen Einstellungen wie etwa via `/etc/rpmrc` vorgenommen wurden):

`SOURCES` für die originalen Quellen (`.tar.gz`-Dateien etc.) und für die distributionsspezifischen Anpassungen (`.dif`-Dateien).

`SPECS` für die `.spec`-Dateien, die in der Art eines Meta-Makefiles den build-Prozess steuern.

`BUILD` unterhalb dieses Verzeichnisses werden die Quellen entpackt, gepatcht und kompiliert.

`RPMS` hier werden die fertigen Binary-Pakete abgelegt.

`SRPMS` und hier die Source-RPMs.

Wenn Sie ein Quellpaket mit YaST installieren, dann werden die für den build-Prozess notwendigen Komponenten unter `/usr/src/packages` installiert: die Quellen und die Anpassungen unter `SOURCES` und die dazugehörige `.spec`-Datei unter `SPECS`.

Hinweis

Bitte machen Sie keine RPM-Experimente mit wichtigen System-Komponenten (`glibc`, `rpm`, `sysvinit` etc.), Sie setzen damit die Funktionstüchtigkeit Ihres Systems aufs Spiel.

Hinweis

Im Folgenden wird das Paket `wget.src.rpm` betrachtet. Nachdem das Quellpaket `wget.src.rpm` mit YaST installiert wurde, gibt es die Dateien:

```
/usr/src/packages/SPECS/wget.spec
/usr/src/packages/SOURCES/wget-1.4.5.dif
/usr/src/packages/SOURCES/wget-1.4.5.tar.gz
```

Mit `rpmbuild -b X /usr/src/packages/SPECS/wget.spec` wird der Kompiliervorgang angestoßen; dabei kann `X` für verschiedene Stufen stehen (vgl. die `--help`-Ausgabe bzw. die RPM-Dokumentation); hier nur eine kurze Erläuterung:

`-bp` Quellen im Verzeichnis `/usr/src/packages/BUILD` präparieren: entpacken und patchen

`-bc` wie `-bp`, jedoch zusätzlich noch kompilieren

`-bi` wie `-bc`, jedoch zusätzlich noch installieren; Achtung, wenn ein Paket nicht das BuildRoot-Feature unterstützt, ist es möglich, dass Sie sich während dieses Installationsvorgangs wichtige Konfigurationsdateien überschreiben!

`-bb` wie `-bi`, jedoch zusätzlich noch das sog. Binary-RPM herstellen; bei Erfolg liegt es in `/usr/src/packages/RPMS`.

`-ba` wie `-bb`, jedoch zusätzlich noch das sog. Source-RPM herstellen; bei Erfolg liegt es in `/usr/src/packages/SRPMS`.

`--short-circuit` Mit dieser Option lassen sich einzelne Schritte überspringen.

Das erzeugte Binary-RPM ist schließlich mit `rpm -i` oder besser mit `rpm -U` zu installieren.

5.3.6 RPM-Pakete mit build erzeugen

Bei vielen Paketen besteht die Gefahr, dass während ihrer Erstellung ungewollt Dateien in das laufende System kopiert werden. Um dies zu vermeiden, können Sie das `build` verwenden, das eine definierte Umgebung herstellt, in der das Paket gebaut wird. Zum Aufbau dieser chroot-Umgebung muss dem `build` Skript ein kompletter Paketbaum zur Verfügung stehen. Dieser kann auf Festplatte, über NFS oder auch von DVD bereitgestellt werden. Dem Skript teilt man die entsprechende Stelle mit dem Befehl `build --rpms <Pfad>` mit. Im Unterschied zu `rpm` möchte der Befehl `build` das SPEC-File im gleichen Verzeichnis haben, wie die eigentlichen Quellen. Wenn Sie wie im obigen Beispiel wget neu übersetzen möchten, und die DVD unter `/media/dvd` in das System eingehängt ist, verwenden Sie als Benutzer `root` folgende Befehle:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Daraufhin wird unter `/var/tmp/build-root` eine minimale Umgebung aufgebaut, in der das Paket gebaut wird. Die entstandenen Pakete liegen danach in `/var/tmp/build-root/usr/src/packages/RPMS`

Das `build` Skript stellt noch einige weitere Optionen zur Verfügung. So kann man eigene RPMs bevorzugt verwenden lassen, die Initialisierung der Build-Umgebung auslassen oder den `rpm`-Befehl auf eine der bereits beschriebenen Stufen beschränken. Sie erhalten mehr Informationen mit dem Befehl `build --help` und in der Manpage `man build`.

5.3.7 Tools für RPM-Archive und die RPM-Datenbank

Der Midnight Commander (`mc`) kann den Inhalt eines RPM-Archivs anzeigen bzw. Teile daraus kopieren. Er bildet ein solches Archiv als ein virtuelles Dateisystem ab, sodass alle gewohnten Menüpunkte des Midnight Commander – wenn sinnvoll – zur Verfügung stehen: Die Informationen in den Kopfzeilen der Datei `HEADER` kann man sich mit (F3) ansehen; mit den Cursor-Tasten und (Enter) lässt sich durch die Struktur des Archivs browsen, um bei Bedarf mit (F5) Komponenten herauszukopieren.

KDE enthält das Tool kpackage, bei GNOME finden Sie gnorpm.

Mit Alien (`alien`) ist es möglich, die Paketformate der verschiedenen Distributionen zu konvertieren. So kann man versuchen, alte TGZ-Archive *vor* dem Installieren nach RPM umzuwandeln, damit *während* der Installation die RPM-Datenbank mit den Paket-Informationen versorgt wird. Aber Achtung: `alien` ist ein Perl-Skript und befindet sich nach Angaben der Programm-Autoren noch in einem Alpha-Stadium – wenngleich es bereits eine hohe Versionsnummer erreicht hat. Übrigens, mittlerweile gibt es auch für den Emacs ein `rpm.el`, ein Frontend für rpm.

Systemreparatur

SUSE LINUX Enterprise Server bietet neben zahlreichen YaST-Modulen zur Systeminstallation und -konfiguration auch Funktionalität zur Reparatur des installierten Systems. Dieses Kapitel beschreibt die verschiedenen Arten und Stufen der Systemreparatur.

6.1 Starten der YaST-Systemreparatur 204
6.2 Automatische Reparatur 205
6.3 Benutzerdefinierte Reparatur 206
6.4 Expertenwerkzeuge 207
6.5 S/390, zSeries: Die initrd als Rettungssystem . . . 208

6.1 Starten der YaST-Systemreparatur

Weil im Schadensfall nicht sicher davon ausgegangen werden kann, dass Ihr System überhaupt noch bootet, und weil ein gerade laufendes System ohnehin schlecht repariert werden kann, wird die YaST-Systemreparatur über das SUSE LINUX Installationsmedium gestartet. Nachdem Sie die im Kapitel 1 auf Seite 7 genannten Schritte durchlaufen haben, gelangen Sie in den Dialog zur Auswahl der Installationsart und wählen dort bitte die Option 'Reparatur des installierten Systems' (Abb. 6.1).

Hinweis

Auswahl des Installationsmediums

Für den Test und die Reparatur werden Treiber vom Installationsmedium geladen. Sie müssen daher darauf achten, ein Installationsmedium zu verwenden, das *genau* zu Ihrer installierten Version von SUSE LINUX passt.

Hinweis

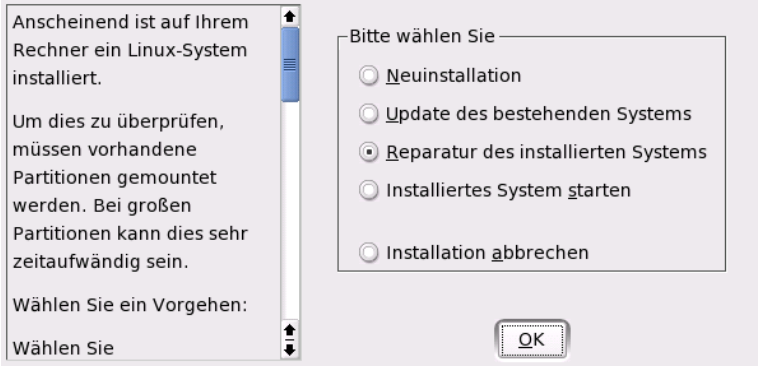

Abbildung 6.1: *Auswählen der YaST-Systemreparatur*

Danach wählen Sie aus, wie die Reparatur des Systems durchgeführt werden soll. Folgende Möglichkeiten stehen zur Auswahl und werden nachfolgend beschrieben.

- Automatische Reparatur
- Benutzerdefinierte Reparatur
- Expertenwerkzeuge

6.2 Automatische Reparatur

Bei unklarer Fehlersituation ist diese Methode am besten geeignet, ein beschädigtes System wieder herzustellen. Nach der Auswahl beginnt eine ausführliche Analyse des installierten Systems, die aufgrund der Vielzahl von Prüfungen und Untersuchungen einige Zeit in Anspruch nimmt. Der Fortschritt dieses Vorgangs wird am unteren Bildschirmrand anhand zweier Fortschrittsbalken dargestellt. Der obere zeigt den Ablauf der aktuell ausgeführten Teilprüfung, während der untere den Fortschritt der gesamten Untersuchung anzeigt. Im Logging-Fenster darüber können Sie verfolgen, welche Aktion gerade stattfindet und welches Ergebnis die jeweilige Prüfung hatte (Abb. 6.2 auf der nächsten Seite). Die folgenden Testgruppen werden durchgeführt, wobei jede Gruppe noch eine Vielzahl untergeordneter Einzelprüfungen beinhaltet.

Partitionstabellen aller Festplatten
Die Gültigkeit und Konsistenz der Partitionstabellen aller gefundenen Festplatten wird geprüft.

Swap-Bereiche Die Swap-Bereiche des installierten Systems werden gesucht, geprüft und ggf. zur Aktivierung angeboten. Sie sollten der Aktivierung zustimmen, weil dadurch die Geschwindigkeit der YaST-Systemreparatur gesteigert wird.

Dateisysteme Für alle gefundenen Dateisysteme wird eine Dateisystem-spezifische Prüfung durchgeführt.

Einträge der Datei `/etc/fstab` Es wird geprüft, ob die Einträge in der Datei vollständig und konsistent sind. Alle gültigen Partitionen werden eingebunden.

Bootloader-Konfiguration Die Bootloader-Konfiguration des installierten Systems (GRUB oder LILO) wird auf Vollständigkeit und Konsistenz geprüft. Boot- und Root-Device werden untersucht und die Verfügbarkeit der initrd-Module kontrolliert.

Paketdatenbank Es wird geprüft, ob alle Pakete vorhanden sind, die zum Betrieb einer Minimal-Installation notwendig sind. Wahlweise können auch die Basispakete analysiert werden, jedoch dauert diese Untersuchung wegen des großen Umfangs recht lange.

Wenn ein Fehler gefunden wird, stoppt die Analyse und ein Dialog wird geöffnet, der Details anzeigt und Lösungsmöglichkeiten anbietet. Aufgrund der Vielzahl von Prüfungen ist es hier nicht möglich, auf all diese

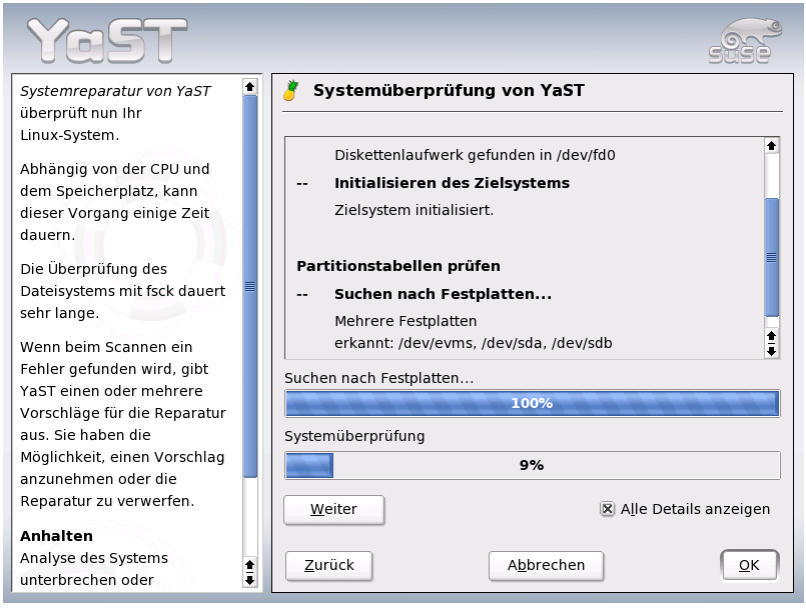

Abbildung 6.2: *Der automatische Reparaturmodus*

Fälle einzugehen. Bitte lesen Sie die Hinweise am Bildschirm genau und wählen Sie dann aus den angebotenen Optionen die gewünschte aus. In Zweifelsfällen können Sie die vorgeschlagene Reparatur natürlich auch ablehnen. Das System bleibt dann in diesem Punkt unverändert. Es wird in keinem Fall automatisch und ohne Rückfrage repariert.

6.3 Benutzerdefinierte Reparatur

Die im vorigen Abschnitt erklärte automatische Reparatur führt kategorisch alle Tests durch. Dies ist sinnvoll, wenn völlig unklar ist, was genau im installierten System beschädigt ist. Wenn Sie jedoch bereits wissen, welcher Systembereich betroffen ist, können Sie hier die Anzahl der durchgeführten Tests einschränken. Nach Auswahl von 'Benutzerdefinierte Reparatur' erhalten Sie eine Auswahl von Testgruppen, die zunächst alle angewählt sind. Der Gesamtumfang der Prüfungen ist damit der gleiche wie bei der automatischen Reparatur. Wenn Sie bereits wissen, wo sich der Fehler

sicher *nicht* befindet, können Sie die entsprechenden Gruppen durch einen Klick auf die zughörige Checkbox abwählen. Nach einem Klick auf 'Weiter' startet dann eine reduzierte Testprozedur mit gegebenenfalls deutlich kürzerer Laufzeit. Beachten Sie dabei jedoch, dass nicht alle Testgruppen einzeln anwendbar sind. Die Prüfung der fstab-Einträge ist z.B. immer mit einer Prüfung der Dateisysteme einschließlich vorhandener Swap-Bereiche verbunden. Falls nötig bereinigt YaST solche Abhängigkeiten durch automatische Anwahl der kleinstmöglichen Anzahl von Testgruppen.

6.4 Expertenwerkzeuge

Wenn Sie sich mit SUSE LINUX gut auskennen und schon eine sehr konkrete Vorstellung davon haben, was in Ihrem System repariert werden muss, können Sie nach Auswahl von 'Expertenwerkzeuge' gezielt jenes Werkzeug anwenden, das Sie für die Reparatur benötigen.

Neuen Bootloader installieren Hier starten Sie das YaST-Bootloader-Konfigurationsmodul. Details hierzu finden Sie im Kapitel 8.6 auf Seite 244

Partitionierer starten Hier starten Sie den YaST-Expertenpartitionierer. Details hierzu finden Sie im Kapitel 1.7.5 auf Seite 24

Reparatur des Dateisystems Hier können Sie die Dateisysteme Ihres installierten Systems prüfen. Sie erhalten zunächst eine Auswahl aller gefundenen Partionen und können dort jene auswählen, die Sie prüfen möchten.

Verlorene Partitionen wieder herstellen
Wenn Partitionstabellen in Ihrem System beschädigt sind, können Sie hier eine Rekonstruktion versuchen. Bei mehreren Festplatten bekommen Sie zunächst Gelegenheit, eine davon auszuwählen. Nach einem Klick auf 'OK' beginnt dann die Prüfung. Dies kann je nach Rechenleistung und Größe der Festplatte einige Zeit dauern.

Hinweis

Rekonstruktion der Partitionstabelle

Die Rekonstuktion einer Partitionstabelle ist schwierig. YaST versucht, durch Analyse des Festplatten-Datenbereiches verlorene Partitionen zu erkennen. Bei Erfolg werden sie in die rekonstruierte Partitionstabelle aufgenommen. Dies gelingt aber nicht in allen denkbaren Fällen.

Hinweis

Systemeinstellungen auf Diskette speichern
Mit dieser Option können Sie wichtige Systemdateien auf eine Diskette sichern. Falls dann später einmal eine dieser Dateien beschädigt ist, kann sie von der Diskette wieder restauriert werden.

Installierte Software prüfen Hier wird die Konsistenz der Paketdatenbank getestet und die Verfügbarkeit der wichtigsten Pakete geprüft. Sollten installierte Pakete beschädigt sein, können Sie hier deren Neuinstallation veranlassen.

6.5 S/390, zSeries: Die initrd als Rettungssystem

Wenn der Kernel des SUSE LINUX Enterprise Servers für S/390 und zSeries aktualisiert oder geändert wurde, kann es vorkommen, dass das System bei einem Reboot in einem inkonistenten Zustand hochfährt und alle Standardverfahren zum IPL des installierten Systems versagen. Meistens tritt diese Situation auf, wenn der Kernel aktualisiert wurde, aber zipl anschließend nicht ausgeführt wurde, um den IPL-Record zu aktualiseren. Dieses Kapitel beschreibt, wie das Standard Installationspaket als Rettungssystem eingesetzt werden kann, von dem zipl ausgeführt werden kann, um den IPL-Record zu aktualisieren.

6.5.1 IPL des Rettungssystems

Hinweis

Bereitstellen der Installationsdaten

Damit diese Methode angewandt werden kann, müssen die Installationsdaten des SUSE LINUX Enterprise Servers verfügbar sein. Details hierzu schlagen Sie im Kapitel *Bereitstellen der Installationsdaten* des *Architekturspezifika* Handbuches nach. Zusätzlich benötigen Sie die Channel Number des Geräts und die Partitionsnummer auf dem Gerät, auf dem sich das Rootfilesystem der SUSE LINUX Enterprise Server-Installation befindet.

Hinweis

Führen Sie zuerst den IPL des SUSE LINUX Enterprise Servers wie im *Architekturspezifika* Handbuch beschrieben durch. Anschließend wird Ihnen eine Liste zur Auswahl eines Netzwerkadapters ausgegeben.

Beispiel 6.1: *Auswahl des Netzwerktyps*

```
=                                                    =
==-  Welcome to SUSE LINUX Server 8 for zSeries     -==
=                                                    =

Please select the type of your network device:
 0) no network
 1) OSA Token Ring
 2) OSA Ethernet
 3) OSA-Gigabit Ethernet or OSA-Express Fast Ethernet
 4) Channel To Channel
 5) Escon
 6) IUCV
 8) Hipersockets
 9) OSA High speed Token Ring (qdio)
10) Show subchannels and detected devices
Enter your choice (0-10):
```

Wählen Sie `0` für *no network* aus. Das Installationsprogramm wird beendet und die folgenden Meldungen ausgegeben:

Beispiel 6.2: *Ausgabe bei nicht selektiertem Netzwerkadapter*

```
*** OK, NETWORK ACCESS WILL _NOT_ BE AVAILABLE. ***


You should be able to login via ssh now.
To restart network setup, enter:

netsetup

To continue the installation, enter:

./inst_source

bash: no job control in this shell
SuSE Instsys suse:/ #
```

Jetzt öffnet sich eine Rootshell, von der aus die benötigten Kommandos direkt eingegeben werden können.

6.5.2 Laden der DASD-Module

Um auf das Rootdevice zugreifen zu können, müssen die benötigten Kernelmodule geladen werden. Zuerst müssen die DASD-Module geladen werden. Sie setzen sich aud einem „middle layer module“ `dasd_mod` und einem „low-level module“, das vom DASD-Typ abhängig ist, zusammen. In diesem Fall werden ECKD-Geräte angenommen, also heisst das entsprechende Modul `dasd_eckd_mod`. Das `dasd_mod` Modul benötigt die Channelbereiche der DASDs, auf die der Zugriff erfolgen soll, als Argument (z.B. `0150`). Die Module werden mittels der folgenden Kommandos geladen:

Beispiel 6.3: *Laden von DASD Modulen*

```
SuSE Instsys suse:/ # insmod dasd_mod dasd=0150
Using /lib/modules/version/kernel/drivers/s390/block/dasd_mod.o
dasd: initializing...
debug: dasd: new level 3
dasd: Registered successfully to major no 94
dasd: initialization finished
SuSE Instsys suse:/ # insmod dasd_eckd_mod
Using /lib/modules/version/kernel/drivers/s390/block/dasd_eckd_mod.o
```

```
dasd(eckd): ECKD discipline initializing
[ ... ]
Partition check:
 dasda:VOL1/  0X0150: dasda1 dasda2
dasd(eckd): We are interested in: CU 3880/00
dasd(eckd): We are interested in: CU 3990/00
dasd(eckd): We are interested in: CU 2105/00
dasd(eckd): We are interested in: CU 9343/00
```

Wenn die Zeile `Partition check` ausgegeben wird, sind alle Module korrekt geladen und das DASD zum Mounten bereit.

6.5.3 Mounten des Rootdevices

Falls alle Module korrekt geladen wurden, können Sie nun das Rootdevice mounten. Angenommen das Rootdevice befindet sich in der zweiten Partition auf dem DASD (`/dev/dasda2`), lautet das entsprechende Kommando folgendermaßen:

Beispiel 6.4: *Mounten des Rootdevices*

```
SuSE Instsys suse:/ # mount /dev/dasda2 /mnt
```

Hinweis

Konsistenz des Dateisystems

Wurde das installierte System nicht sauber heruntergefahren, kann es ratsam sein, die Konsistenz des Dateisystems vor dem Mounten zu überprüfen. So wird Datenverlust vermieden. Im Beispiel verwenden Sie das Kommando `fsck /dev/dasda2`, um das Dateisystem auf Konsistenz zu prüfen.

Hinweis

Mit Eingabe von `mount` überprüfen Sie, ob das Dateisystem korrekt gemountet wurde.

Beispiel 6.5: *Ausgabe des mount Kommandos*

```
SuSE Instsys suse:/ # mount
shmfs on /newroot type shm (rw,nr_inodes=10240)
devpts on /dev/pts type devpts (rw)
virtual-proc-filesystem on /proc type proc (rw)
/dev/dasda2 on /mnt type reiserfs (rw)
```

6.5.4 Wechsel in das gemountete Dateisystem

Damit zipl seine Konfiguration vom Rootdevice des installierten Systems und nicht vom Rettungssystem einliest, wechseln Sie zum Rootdevice des installierten Systems. Diesen Wechsel nehmen Sie mit `chroot` vor:

Beispiel 6.6: *chroot in das gemountete Dateisystem*

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

6.5.5 Ausführen von zipl

Führen Sie nun das Kommando `zipl` aus, um den IPL-Record mit den korrekten Werten erneut zu schreiben:

Beispiel 6.7: *Installieren des IPL-Records mit zipl*

```
sh-2.05b# zipl
building bootmap : /boot/zipl/bootmap
adding Kernel Image : /boot/kernel/image located at 0x00010000
adding Ramdisk : /boot/initrd located at 0x00800000
adding Parmline : /boot/zipl/parmfile located at 0x00001000
Bootloader for ECKD type devices with z/OS compatible layout install
Syncing disks....
...done
```

6.5.6 Verlassen des Rettungssystems

Um das Rettungssystem zu verlassen, verlassen Sie zuerst die Shell, die mit dem `chroot` Kommando geöffnet wurde:

Beispiel 6.8: *Verlassen der „chrooted“ Shell*

```
sh-2.05b# exit
exit
SuSE Instsys suse:/mnt #
```

Um Datenverlust zu vermeiden, schreiben Sie mithilfe des `sync` Kommandos alle ungeschriebenen Puffer auf die Festplatte. Nun wechseln Sie in das Rootverzeichnis des Rettungssystems und hängen das Rootdevice der SUSE LINUX Enterprise Server Installation aus.

Beispiel 6.9: *Unmounten des Dateisystems*

```
SuSE Instsys suse:/mnt # cd /
SuSE Instsys suse:/ # umount /mnt
```

Zum Schluss halten beenden Sie das Rettungssystem mit dem `halt` Kommando an. Der IPL des SUSE LINUX Systems kann nun wie in Abschnitt 1.7.11 auf Seite 37 beschrieben vorgenommen werden.

Teil II

System

32-bit und 64-bit Applikationen in einer 64-bit Systemumgebung

SUSE LINUX Enterprise Server ist für mehrere 64-bit Plattformen erhältlich. Dies bedeutet nicht notwendigerweise, dass alle enthaltenen Applikationen schon auf 64-bit portiert wurden. SUSE LINUX Enterprise Server unterstützt die Verwendung von 32-bit Applikationen in einer 64-bit Systemumgebung. Dieses Kapitel gibt Ihnen einen kleinen Überblick, wie diese Unterstützung auf 64-bit SUSE LINUX Enterprise Server Plattformen umgesetzt wird.

7.1 Laufzeit-Unterstützung 218
7.2 Softwareentwicklung 219
7.3 Software-Kompilierung auf Biarch-Plattformen . . 220
7.4 Kernel-Spezifika 222

SUSE LINUX Enterprise Server für die 64-bit Plattformen ipf, ppc64, s390x, sparc64, amd64 und em64t ist so ausgelegt, dass existierende 32-bit Applikationen in der 64-bit Umgebung „out-of-the-box“ lauffähig sind. Die entsprechenden 32-bit Plattformen sind x86 für ipf, ppc für ppc64, s390 für s390x und x86 für amd64 und em64t. Dank dieser Unterstützung ist es möglich, Ihre bevorzugten 32-bit Applikationen weiter zu verwenden, ohne dass Sie auf die Verfügbarkeit eines entsprechenden 64-bit-Ports warten müssten. Das aktuelle ppc64 System läuft im 32-bit Modus, während Sie 64-bit Applikationen verwenden können.

Um die 32-bit Unterstützung zu verstehen, müssen wir uns mit folgenden Themen auseinandersetzen:

Laufzeit-Unterstützung Wie können 32-bit Applikationen ausgeführt werden?

Entwicklungs-Unterstützung Wie müssen 32-bit Applikationen kompiliert werden, damit sie sowohl in 32-bit als auch 64-bit Systemumgebungen lauffähig sind?

Kernel API Wie können 32-bit Applikationen unter einem 64-bit Kernel laufen?

7.1 Laufzeit-Unterstützung

Hinweis

Konflikte zwischen 32-bit und 64-bit Version einer Applikation

Ist eine Applikation sowohl für 32-bit als auch für 64-bit verfügbar, wird eine parallele Installation beider Versionen zwangsläufig Probleme bereiten. In solchen Fällen müssen Sie sich auf eine der beiden Versionen festlegen und diese installieren und verwenden.

Hinweis

Jede Applikation benötigt eine Reihe von Bibliotheken, um korrekt ausgeführt zu werden. Leider sind die Bezeichnungen für die 32-bit und 64-bit Versionen dieser Bibliotheken identisch – sie müssen auf eine andere Art und Weise voneinander unterschieden werden.

Für die 64-bit Plattformen ppc64, s390x, sparc64, amd64 und em64t wird ein und derselbe Ansatz verwendet: Um die Kompatibilität mit der 32-bit

Version zu erhalten, werden die Bibliotheken an derselben Stelle im System gespeichert, an der sie auch in der 32-bit Umgebung liegen. Die 32-bit Version der `libc.so.6` befindet sich sowohl in der 32-bit als auch der 64-bit Umgebung unter `/lib/libc.so.6`.

Alle 64-bit Bibiliotheken und Objektdateien sind in Verzeichnissen namens `lib64/`, d.h. dass die 64-bit Objektdateien, die Sie normalerweise unter `/lib/`, `/usr/lib/` und `/usr/X11R6/lib/` suchen würden, nun unter `/lib64/`, `/usr/lib64/` und `/usr/X11R6/lib64/` zu finden sind. So ist für die 32-bit Bibliotheken Platz unter `/lib/`, `/usr/lib/` und `/usr/X11R6/lib/`, wobei der Dateiname für beide Versionen unverändert beibehalten werden kann.

Grundsätzlich wurden Unterverzeichnisse der Objektverzeichnisse, deren Dateninhalt von der Wortgröße unabhängig ist, *nicht* verschoben. Sie werden beispielsweise die X11 Fonts weiterhin wie gewöhnlich unter `/usr/X11R6/lib/X11/fonts` finden.

Dieses Schema ist mit der LSB (Linux Standards Base) und dem FHS (File System Hierarchy Standard) konform.

► **IPF**
Für ipf, ebenso für die 64-bit Alpha Plattform, liegen die 64-bit Bibliotheken in den standardmäßigen `lib/` Verzeichnissen. In diesen Fällen gibt es weder ein `lib64/` noch ein `lib32/` Verzeichnis. Stattdessen führt ipf den 32-bit x86 Code unter einer Emulation aus. Ein Satz von Basisbibliotheken ist in `/emul/ia32-linux/lib/` und `/emul/ia32-linux/usr/X11R6/lib/` installiert. ◄

7.2 Softwareentwicklung

Alle 64-bit Architekturen unterstützen die Entwicklung von 64-bit Objekten. Der Unterstützungsgrad für 32-bit Kompilierung hängt allerdings von der Architektur ab. Dies sind die unterschiedlichen Realisierungsmöglichkeiten für die Toolchain aus GCC (GNU Compiler Collection) und Binutils, die den Assembler as und den Linker ld umfassen:

Biarch Compiler Mit einer Biarch-Development-Toolchain können sowohl 32- als auch 64-bit Objekte generiert werden. Auf fast allen Plattformen ist der Standard die Kompilierung von 64-bit Objekten. Wenn spezielle Flags verwendet werden, können 32-bit Objekte generiert werden. Für GCC ist dieses spezielle Flag `-m32` (bzw. für s390x `-m31`). Für die Binutils sind diese Flags architekturabhängig. GCC

wird die korrekten Flags aber an Linker und Assembler übergeben. Eine Biarch-Development-Toolchain existiert im Moment für sparc64 (unterstützt sparc und sparc64 Entwicklung), für amd64 (unterstützt die Entwicklung für x86 und amd64 Instruktionen), für s390x und für ppc64. Auf der ppc64-Plattform werden normalerweise 32-bit Objekte erzeugt. Um 64-bit Objekte zu generieren, muss das Flag `-m64` verwendet werden.

Keine Unterstützung SUSE unterstützt nicht die direkte Entwicklung von 32-bit Software auf allen Plattformen. Sollten Sie unter ipf Applikationen für x86 entwickeln wollen, müssen Sie die entsprechende 32-bit Version des SUSE LINUX Enterprise Servers verwenden.

Beachten Sie, dass alle Headerdateien in einer architektuunabhängigen Form geschrieben werden müssen und dass die installierten 32- und 64-bit Bibliotheken eine API (Application Programming Interface) aufweisen müssen, die zu den installierten Headerdateien passt. Die normale SUSE-Umgebung ist nach diesem Schema konzipiert – für selbst aktualisierte Bibliotheken müssen Sie sich selbst um diese Belange kümmern.

7.3 Software-Kompilierung auf Biarch-Plattformen

Um auf einer Biarch-Architektur Binaries für die jeweils andere Architektur zu entwickeln, müssen Sie die entsprechenden Bibliotheken für die Zweitarchitektur zusätzlich installieren. Diese Pakete heissen `rpmname-32bit`, wenn die Zweitarchitektur eine 32-bit Architektur ist bzw. `rpmname-64bit`, wenn die Zweitarchitektur eine 64-bit Architektur ist.

Ausserdem benötigen Sie die entsprechenden Header und Bibliotheken, die Sie in den `rpmname-devel`-Paketen finden, sowie die Entwicklungsbibliotheken zur Zweitarchitektur, die entsprechend entweder unter `rpmname-devel-32bit` oder `rpmname-devel-64bit` zu finden sind.

Wenn Sie zum Beispiel ein Programm kompilieren, dass `libaio` auf einem System, dessen Zweitarchitektur 64-bit hat, verwendet, benötigen Sie die folgenden RPMs:

libaio 32-bit Laufzeitpaket

libaio-devel Header und Bibliotheken für die 32-bit Entwicklung

libaio-64bit 64-bit Laufzeitpaket

libaio-devel-64bit 64-bit Entwicklungsbibliotheken

Die meisten Opensource Programme verwenden eine autoconf-basierte Programmkonfiguration. Um autoconf zur Konfiguration eines Programms für die Zweitarchitektur einzusetzen, müssen Sie die normalen Compiler- und Linkereinstellungen von autoconf durch einen Aufruf des configure Skripts mit zusätzlichen Umgebungsvariablen überschreiben.

Das folgende Beispiel bezieht sich auf ein ppc System mit ppc64 als Zweitarchitektur:

- Legen Sie fest, dass autoconf den 64-bit Compiler verwenden soll:

  ```
  CC="gcc -m64"
  ```

- Weisen Sie den Linker an, 64-bit Objekte zu verarbeiten:

  ```
  LD="ld -m elf64ppc"
  ```

- Legen Sie fest, dass der Assembler 64-bit Objekte erzeugt:

  ```
  AS="gcc -c -m64"
  ```

- Legen Sie fest, dass die Bibliotheken für libtool etc. aus `/usr/lib64/` stammen:

  ```
  LDFLAGS="-L/usr/lib64"
  ```

- Legen Sie fest, dass die Bibliotheken im `lib64`-Unterverzeichnis abgelegt werden:

  ```
  --libdir=/usr/lib64
  ```

- Legen Sie fest, dass die 64-bit X-Bibliotheken verwendet werden:

  ```
  --x-libraries=/usr/X11R6/lib64/
  ```

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie den Gegebenheiten des Programms an.

Ein beispielhafter `configure`-Aufruf könnte folgendermaßen aussehen:

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
        .configure       \
           --prefix=/usr \
           --libdir=/usr/lib64
make
make install
```

7.4 Kernel-Spezifika

Die 64-bit Kernel für ppc64, s390x, amd64 und em64t bieten sowohl eine 64- als auch eine 32-bit Kernel-ABI (Application Binary Interface). Die Letztere ist identisch mit der ABI für den entsprechenden 32-bit Kernel. Dies bedeutet, dass die 32-bit Applikation mit dem 64-bit Kernel auf gleiche Weise kommunizieren kann wie mit dem 32-bit Kernel.

Bitte beachten Sie, dass die 32-bit Emulation von Systemaufrufen eines 64-bit Kernels eine Anzahl von APIs nicht unterstützt, die von Systemprogrammen verwendet werden. Dies ist von der Plattform abhängig. Aus diesem Grund müssen einige wenige Anwendungen wie lspci oder die LVM-Verwaltungsprogramme auf nicht-ppc64-Plattformen als 64-bit Programme existieren, wenn sie korrekt funktionieren sollen.

Ein 64-bit Kernel kann ausschließlich 64-bit Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. Die Verwendung von 32-bit Kernel-Modulen ist *nicht* möglich.

Hinweis

Einige Applikationen benötigen eigene kernel-ladbare Module. Sollten Sie vorhaben, eine solche 32-bit Applikation in einer 64-bit Systemumgebung zu verwenden, kontaktieren Sie den Anbieter dieser Applikation und SUSE, um sicherzugehen, dass die 64-bit Version des kernel-ladbaren Moduls und die 32-bit Übersetzung der Kernel API für dieses Modul verfügbar sind.

Hinweis

Booten und Bootmanager

Im Folgenden werden verschiedene Methoden zum Booten des fertig installierten System vorgestellt. Um das Verständnis der einzelnen Methoden zu erleichtern, werden zunächst einige technische Details des Bootprozesses erläutert. Im Anschluss daran folgen Erläuterungen zum aktuell verwendeten Bootmanager GRUB und seinem Vorgänger LILO.

Dieses Kapitel bezieht sich ausschließlich auf die Prozessorarchitekturen AMD64, x86 und Intel EM64T.

8.1 Der Bootvorgang auf dem PC 224
8.2 Bootkonzepte 225
8.3 Map Files, GRUB und LILO 226
8.4 Booten mit GRUB 227
8.5 Booten mit LILO 238
8.6 Bootloader-Konfiguration mit YaST 244
8.7 Linux-Bootloader entfernen 249
8.8 Für alle Fälle: Boot-CD erstellen 250
8.9 S/390, zSeries: Der Bootloader ZIPL 252

8.1 Der Bootvorgang auf dem PC

Nach dem Einschalten des Rechners werden vom BIOS (engl. *Basic Input Output System*) Bildschirm und Tastatur initialisiert sowie der Hauptspeicher getestet. Bis zu diesem Zeitpunkt verfügt der Rechner über keine Massenspeichermedien.

Anschließend werden Informationen über aktuelles Datum, Zeit und die wichtigsten Peripheriegeräte aus den CMOS-Werten (*CMOS Setup*) ausgelesen. Da nun die erste Festplatte einschließlich ihrer Geometrie bekannt sein sollte, kann das Laden des Betriebssystems von dort beginnen.

Dazu wird von der ersten Festplatte der physikalisch erste Datensektor von 512 Byte Größe in den Speicher geladen und die Kontrolle geht auf das Programm zu Beginn dieses Sektors über. Die Abfolge der auf diese Weise ausgeführten Anweisungen bestimmt den weiteren Ablauf des Bootvorgangs. Die ersten 512 Byte auf der ersten Festplatte werden deshalb auch als *Master Boot Record* bezeichnet.

Bis zu diesem Zeitpunkt (Laden des MBR) läuft der Bootvorgang völlig unabhängig vom installierten System auf jedem PC immer gleich ab und der Computer hat bis dahin für den Zugriff auf die Peripherie lediglich die im BIOS gespeicherten Routinen (Treiber) zur Verfügung.

8.1.1 Master Boot Record

Die Struktur des MBR ist durch eine betriebssystemübergreifende Konvention festgelegt. Die ersten 446 Byte sind für Programmcode reserviert. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen; siehe Abschnitt 3.9 auf Seite 148. Ohne die Partitionstabelle gibt es keine Dateisysteme, d.h. die Festplatte ist praktisch nicht zu verwenden. Die letzten zwei Byte müssen eine feste „magische Zahl“ (AA55) enthalten: ein MBR, der dort etwas anderes stehen hat, wird vom BIOS und von allen PC-Betriebssystemen als ungültig angesehen.

8.1.2 Bootsektoren

Bootsektoren sind die jeweils ersten Sektoren der Festplatten-Partitionen, außer bei der erweiterten Partition, die nur ein „Behälter“ für andere Partitionen ist. Diese Bootsektoren bieten 512 Byte Platz und sind dazu gedacht, Code aufzunehmen, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-,

Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Grunddaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen auch nach der Anlage eines Dateisystems erst einmal leer. Eine Linux-Partition ist daher *nicht von selbst startbar*, auch wenn sie einen Kernel und ein gültiges Root-Dateisystem enthält.

Ein Bootsektor mit gültigem Code für den Systemstart trägt in den letzten 2 Bytes dieselbe „magische“ Kennung wie der MBR (AA55).

8.1.3 Booten von DOS oder Windows

Im DOS-MBR der ersten Festplatte ist ein Partitionseintrag als *aktiv* (engl. *bootable*) gekennzeichnet, was bedeutet, dass dort nach dem zu ladenden System gesucht werden soll. Deshalb muss DOS zwingend auf der ersten Festplatte installiert sein. Der DOS-Programmcode im MBR ist die erste Stufe des Bootloaders (engl. *first stage bootloader*) und überprüft, ob auf der angegebenen Partition ein gültiger Bootsektor vorhanden ist.

Falls dies der Fall ist, kann der Code in diesem Bootsektor als „zweite Stufe“ des Bootloaders (engl. *secondary stage loader*) nachgestartet werden. Dieser lädt nun die Systemprogramme und schließlich erscheint der gewohnte DOS-Prompt bzw. es startet die Benutzeroberfläche von Windows.

Unter DOS lässt sich nur eine einzige primäre Partition als aktiv markieren. Folglich kann das DOS–System nicht auf logischen Laufwerken in einer erweiterten Partition untergebracht werden.

8.2 Bootkonzepte

Das einfachste „Bootkonzept“ betrifft einen Rechner mit einem einzigen Betriebssystem. Die Abläufe in der Startphase in diesem Fall haben wir soeben geschildert. Ein solcher Bootvorgang ist auch für einen Nur–Linux–Rechner denkbar. Dann kann theoretisch auf die Installation eines Bootloaders verzichtet werden, allerdings wäre es so nicht möglich, dem Kernel während des Startens eine Kommandozeile (mit Spezialwünschen zum Startvorgang, zusätzlichen Hardware-Informationen usw.) mitzugeben. Sobald mehr als ein Betriebssystem auf einem Rechner installiert ist, bieten sich verschiedene Bootkonzepte an:

Zusätzliche Systeme von Diskette booten
: Ein Betriebssystem wird von Platte geladen, mit Hilfe von Boot-Disketten können alternativ weitere Betriebssysteme vom Disketten-Laufwerk aus gestartet werden.

- *Bedingung:* Ein bootfähiges Diskettenlaufwerk ist vorhanden.
- *Beispiel:* Sie installieren Linux zusätzlich zu Ihrem Windows–System und starten Linux stets von Bootdiskette.
- *Vorteil:* Sie ersparen sich die Bootloader-Installation.
- *Nachteile:* Sie müssen *sehr* darauf bedacht sein, einen Sicherheitsvorrat funktionierender Bootdisketten zu haben und der Start dauert länger.
- Dass Ihr Linux ohne Bootdiskette nicht starten kann, mag je nach beabsichtigtem Einsatz Ihres Rechners ein Vor- oder Nachteil sein.

Zusätzliche Systeme von einem USB-Speichermedium booten
Ebenso wie von einer Diskette können die zum Booten notwendigen Informationen von einem USB-Speichermedium eingelesen werden.

Installation eines Bootmanagers Ein Bootmanager erlaubt, mehrere Systeme gleichzeitig auf einem Rechner zu halten und sie abwechselnd zu nutzen. Der Benutzer wählt das zu ladende System bereits während des Bootvorgangs aus; ein Wechsel erfordert den Neustart des Rechners. Bedingung ist dabei, dass der gewählte Bootmanager mit allen Betriebssystemen „harmoniert“. Die Bootmanager von SUSE LINUX (LILO und sein Nachfolger GRUB) können alle gängigen Betriebssysteme starten. SUSE LINUX installiert daher den gewünschten Bootmanager standardmäßig in den MBR, so Sie diese Einstellung nicht während des Installationsdialogs ändern.

8.3 Map Files, GRUB und LILO

Das größte Problem beim Booten eines Betriebssystems besteht darin, dass der Kernel eine Datei auf einem Dateisystem auf einer Partition auf einer Festplatte ist. Für das BIOS allerdings sind Dateisysteme und Partitionen völlig unbekannte Konzepte.

Um dieses Problem zu umgehen, wurden so genannte „Maps“ und „Map Files“ eingeführt. In den Maps werden die physikalischen Blöcke auf der Festplatte notiert, die von den logischen Dateien belegt sind. Wenn so eine Map verarbeitet wird, lädt das BIOS die physikalischen Blöcke in der Reihenfolge, wie sie in der Map-Datei angegeben ist, und baut so die logische Datei im Speicher auf.

Im Gegensatz zu LILO, der sich vollständig auf Maps verlässt, versucht GRUB, sich sobald als möglich von den festen Maps zu lösen Dies erreicht GRUB durch *File System Code*, der es ermöglicht, auf Dateien durch die Pfadangabe zuzugreifen und nicht mehr durch die Blocknummern.

Dieser Unterschied hat historische Gründe. In den frühen Tagen von Linux kämpften viele verschieden Dateisysteme um die Vorherrschaft. Werner Almesberger entwickelte einen Bootloader (LILO), der nicht wissen musste, auf welchem Filesystem der zu bootende Kernel angelegt war. Die Idee hinter GRUB geht sogar noch weiter zurück in die Tage des traditionellen Unix und BSD. Diese hatten sich gewöhnlich auf ein Dateisystem festgelegt und am Anfang desselben einen bestimmten Platz für den Bootloader reserviert. Dieser Bootloader kannte die Struktur des Dateisystems, in das er eingebunden war, und fand dort die Kernel mit ihren Namen im root-Verzeichnis.

Hinweis

Wann wird welcher Bootloader installiert?

Wenn Sie ein Update von einer früheren SUSE LINUX Version durchführen, die LILO benutzte, wird auch wieder LILO eingerichtet. Bei einer Neuinstallation wird dagegen GRUB verwendet, außer die Root-Partition wird auf folgenden Raid-Systemen installiert:

- CPU-abhängige Raid-Controller (wie z.B. viele Promise- oder Highpoint Controller)
- Software-Raid
- LVM

Informationen zur Installation und Konfiguration von LILO erhalten Sie unter dem Stichwort „LILO“ in der Support-Datenbank (`http://portal.suse.de/sdb/de/index.html`).

Hinweis

8.4 Booten mit GRUB

GRUB (engl. *Grand Unified Bootloader*) besteht wie LILO aus zwei Stufen. Die erste Stufe (stage1) besteht aus 512 Byte und wird in den MBR oder

den Bootsektor einer Plattenpartition oder Diskette geschrieben. Die zweite, größere Stufe (stage 2) wird im Anschluss daran geladen und enthält den eigentlichen Programmcode. Einzige Aufgabe der ersten Stufe ist bei GRUB, die zweite Stufe des Bootloaders zu laden.

Ab diesem Punkt unterscheidet sich GRUB von LILO. stage2 kann auf Dateisysteme zugreifen. Derzeit werden Ext2, Ext3, ReiserFS, JFS, XFS, Minix und das von Windows verwendete DOS FAT FS unterstützt. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Disk-Devices (Diskette oder vom BIOS erkannte Festplatten) zugreifen, weshalb Änderungen an der GRUB-Konfigurationsdatei keine Neuinstallation des Bootmanagers mehr bedeuten. Beim Booten liest GRUB die Menüdatei samt der aktuellen Pfade und Partitionsangaben zu Kernel oder initialer Ramdisk (`initrd`) neu ein und findet diese Dateien selbständig.

Hinweis

GRUB and JFS

Obwohl technisch möglich, ist eine Kombination von GRUB mit JFS nicht zu empfehlen.

Hinweis

GRUB hat den großen Vorteil, dass alle Bootparameter *vor* dem Booten bequem geändert werden können. Wurde zum Beispiel beim Editieren der Menüdatei ein Fehler gemacht, kann er auf diese Weise „ausgewetzt“ werden. Darüber hinaus können Boot-Kommandos interaktiv über eine Art von Eingabeaufforderung eingegeben werden. GRUB bietet die Möglichkeit, noch vor dem Booten die Lage von Kernel und initrd festzustellen. So booten Sie Betriebssysteme, die noch keinen Eintrag im Bootmenü haben.

8.4.1 Das GRUB-Bootmenü

Hinter dem grafischen Splash-Screen mit dem Bootmenü steht die GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die mit Hilfe des Menüs gebootet werden können.

GRUB liest bei jedem Systemstart die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder erfolgten Änderung an der Datei zu aktualisieren — verwenden Sie einfach YaST oder Ihren favorisierten Editor.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell

durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen vor dem ersten Parameter. Kommentare werden durch einen Hash (#) eingeleitet.

Zur Erkennung der Menüeinträge in der Menü-Übersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als selektierbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrages ausgeführt.

Einfachster Fall ist das Verzweigen zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Boot-Block einer anderen Partition in GRUBs Block-Notation, zum Beispiel:

```
chainloader (hd0,3)+1
```

Die Devicenamen unter GRUB werden in Abschnitt 8.4.1 auf der nächsten Seite erklärt. Obiges Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Kommando `kernel` wird ein Kernel-Image spezifiziert. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel auf der Kommandozeile übergeben.

Wenn der Kernel nicht die erforderlichen Treiber für den Zugriff auf die root-Partition einkompiliert hat, dann muss `initrd` angegeben werden. Hierbei handelt es sich um einen separaten GRUB-Befehl, der den Pfad zur initrd-Datei als einziges Argument hat. Da die Ladeadresse der initrd in das bereits geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den `kernel`-Befehl folgen.

Der Befehl `root` vereinfacht die Spezifikation der Kernel- und initrd-Dateien. `root` hat als einziges Argument entweder ein GRUB-Device oder eine Partition auf einem solchen. Allen Kernel-, initrd- oder anderen Dateipfaden, bei denen nicht explizit ein Device angegeben ist, wird bis zum nächsten `root`-Befehl das Device vorangestellt. In einer `menu.lst`-Datei, die während der Installation generiert wurde, kommt dieser Befehl nicht vor. Er dient der Vereinfachung beim händischen Editieren.

Am Ende jeden Menü-Eintrags steht implizit das `boot`-Kommando, so dass dieses nicht in die Menüdatei geschrieben werden muss. Sollten Sie jedoch in die Situation kommen, GRUB interaktiv zum Booten zu benutzen, müssen Sie am Ende das `boot`-Kommando eingeben. `boot` hat keine Argumente, es führt lediglich das geladene Kernel-Image oder den angegebenen Chain Loader aus.

Wenn Sie alle Menü-Einträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Andernfalls wird der erste (Eintrag `0`) verwendet. Sie haben auch die Möglichkeit, einen Timeout in Sekunden anzugeben, nach dem dies geschehen soll. `timeout` und `default` werden üblicherweise vor die Menüeinträge geschrieben. Eine Beispieldatei samt Erläuterung finden Sie im Abschnitt 8.4.1 auf der nächsten Seite.

Namenskonventionen für Festplatten und Partitionen

GRUB verwendet für die Bezeichnung von Festplatten und Partitionen andere Konventionen, als Sie es von den normalen Linux-Devices (z.B. `/dev/hda1`) her gewohnt sind. Die erste Festplatte wird immer `hd0` genannt, das Diskettenlaufwerk `fd0`.

Hinweis

Partitionzählung in GRUB

Die Zählung der Partitionen in GRUB beginnt bei Null. (`hd0,0`) entspricht der ersten Partition auf der ersten Festplatte; in einem gewöhnlichen Desktop-Rechner mit einer Platte als Primary Master angeschlossen lautet der Device-Name `/dev/hda1`.

Hinweis

Die vier möglichen primären Partitionen belegen die Partitionsnummern `0` bis `3`. Ab `4` werden die logischen Partitionen hochgezählt:

```
(hd0,0)   erste primäre Partition auf der ersten Festplatte
(hd0,1)   zweite primäre Partition
(hd0,2)   dritte primäre Partition
(hd0,3)   vierte primäre (und meist die erweiterte) Partition
(hd0,4)   erste logische Partition
(hd0,5)   zweite logische Partition
...
```

Hinweis

IDE, SCSI oder RAID

GRUB unterscheidet nicht zwischen IDE-, SCSI- oder RAID-Devices. Alle Festplatten, die vom BIOS oder weiteren Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend durchgezählt.

Hinweis

Das Problem, dass Linux-Device-Namen nicht eindeutig zu BIOS-Device-Namen zugeordnet werden können, besteht für sowohl LILO als auch GRUB. Beide benutzen vergleichbare Algorithmen, um diese Zuordnung zu generieren. Jedoch speichert GRUB diese Zuordnung in einer Datei (`device.map`) ab, die bearbeitet werden kann. Mehr Informationen zur Datei `device.map` finden Sie im Abschnitt 8.4.2 auf Seite 234.

Ein kompletter GRUB-Pfad besteht aus einem Device-Namen, der in Klammern geschrieben wird sowie dem Pfad der Datei in dem Dateisystem auf der angegebenen Partition. Der Pfad wird durch einen Slash eingeleitet. Als Beispiel, auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition, könnte der bootbare Kernel wie folgt aussehen:

```
(hd0,0)/boot/vmlinuz
```

Beispiel einer Menü-Datei

Zum besseren Verständnis des Aufbaus einer GRUB-Menüdatei stellen wir ein kurzes Beispiel vor. Diese Beispiel-Installation beinhaltet eine Linux-Bootpartition unter `/dev/hda5`, eine Root-Partition unter `/dev/hda7` und eine Windows-Installation unter `/dev/hda1`.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd
title windows
   chainloader(hd0,0)+1
title floppy
   chainloader(fd0)+1
title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

Der erste Block behandelt die Konfiguration des Splash-Screens:

gfxmenu (hd0,4)/message Das Hintergrundbild liegt auf `/dev/hda5` und trägt den Namen `message`

color white/blue black/light-gray Das Farbschema: weiss (Vordergrund), blau (Hintergrund), schwarz (Auswahl) und hellgrau (Hintergrund der Auswahl). Das Farbschema wirkt sich nicht auf den Splashscreen aus, sondern erst, wenn Sie diesen mit (Esc) verlassen.

default 0 Der erste Menüeintrag mit `title linux` soll standardmäßig gebootet werden.

timeout 8 Nach acht Sekunden ohne Benutzerfeedback bootet GRUB automatisch durch.

Der zweite und größte Block listet die verschiedenen bootbaren Betriebssysteme auf.

- Der erste Eintrag (`title linux`) ist für das Booten von SUSE LINUX zuständig. Der Kernel (`vmlinuz`) liegt auf der ersten Festplatte in den ersten logischen Partition (hier der Bootpartition). Kernelparameter wie zum Beispiel die Angabe der Rootpartition, des VGA-Modus etc. werden hier angehängt. Die Angabe der Rootpartition erfolgt nach dem Linux-Schema (`/dev/hda7/`) da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` liegt ebenfalls in der ersten logischen Partition der ersten Festplatte.
- Der zweite Eintrag ist für das Laden von Windows zuständig. Windows wird von der ersten Partition der ersten Festplatte aus gestartet (`hd0,0`). Mittels `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition gesteuert.
- Der nächste Abschnitt dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu das BIOS umgestellt werden müsste.
- Die Bootoption `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernelparametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden und wird von GRUB automatisch beim nächsten Booten übernommen. Sie können diese Datei mit dem Editor Ihrer Wahl oder mit YaST permanent editieren. Alternativ können Sie temporäre Änderungen interaktiv über die Edit-Funktion von GRUB vornehmen.

Hinweis

Festplattenreihenfolge tauschen

Manche Betriebssysteme (z.B. Windows) können nur von der ersten Festplatte starten. Wenn Sie ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert haben, können Sie beim entsprechenden Menüeintrag einen logischen Tausch veranlassen. Dies funktioniert allerdings nur, wenn das Betriebssystem beim Start über das BIOS auf die Festplatten zugreift.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

Hier soll Windows von der zweiten Festplatte gestartet werden. Dazu wird die logische Reihenfolge der Festplatten mit `map` getauscht. Beachten Sie dabei jedoch, dass sich durch den Tausch die Logik innerhalb der GRUB-Menüdatei *nicht* ändert. Nach wie vor müssen Sie bei `chainloader` die zweite Festplatte angeben.

Hinweis

Ändern von Menü-Einträgen während des Bootvorgangs

Aus dem grafischen Bootmenü von GRUB können Sie mittels der Cursortasten auswählen, welches der verfügbaren Betriebssysteme gestartet werden soll. Wählen Sie ein Linux-System, können Sie am Bootprompt – wie auch von LILO gewohnt – eigene Bootparameter einfügen. GRUB geht noch über dieses Konzept hinaus. Drücken Sie (Esc) und verlassen Sie den Splash-Screen, können Sie nach der Eingabe von (e) (edit) einzelne Menü-Einträge gezielt direkt editieren. Änderungen, die Sie auf diese Weise vornehmen, gelten nur für diesen einen Bootvorgang und werden nicht dauerhaft übernommen.

Hinweis

Tastaturbelegung während des Bootens

Bitte beachten Sie, dass beim Booten nur die amerikanische Tastaturbelegung verfügbar ist. Achten Sie auf die vertauschten Sonderzeichen.

Hinweis

Nach Aktivieren des Editiermodus wählen Sie mittels der Cursortasten den Menü-Eintrag, dessen Konfiguration Sie verändern wollen. Um die Konfiguration editierbar zu machen, geben Sie ein weiteres Mal (e) ein. So korrigieren Sie falsche Partitions- oder Pfadangaben, bevor diese sich negativ auf den Bootprozess auswirken. Mit (Enter) verlassen Sie den Editiermodus, kehren ins Menü zurück und booten diesen Eintrag mit (b). Im Hilfetext am unteren Rand werden weitere Handlungsmöglichkeiten angezeigt.

Möchten Sie geänderte Bootoptionen dauerhaft eintragen, öffnen Sie als Benutzer `root` die Datei `menu.lst` und hängen die zusätzlichen Kernelparameter durch ein Leerzeichen getrennt an die bestehende Zeile an:

```
title linux
kernel (hd0,0)/vmlinuz root=/dev/hda3 <zusätzlicher parameter>
initrd (hd0,0)/initrd
```

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie für diese Änderung auf das YaST-Bootloadermodul aufrufen. Auch hier wird der neue Parameter lediglich durch ein Leerzeichen getrennt an die bestehende Zeile angehängt.

8.4.2 Die Datei device.map

Die schon erwähnte Datei `device.map` enthält die Zuordnungen von GRUB-Devicenamen und Linux-Devicenamen. Sollten Sie ein Mischsystem aus IDE- und SCSI-Festplatten vorliegen haben, muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootreihenfolge zu ermitteln. Die BIOS-Informationen zur Bootreihenfolge sind GRUB nicht zugänglich. Das Ergebnis dieser Überprüfung speichert GRUB unter `/boot/grub/device.map` ab. Eine Beispieldatei `device.map` für ein Beispielsystem – angenommen wird eine im BIOS eingestellte Bootreihenfolge von IDE vor SCSI – sieht so aus:

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/hdb
(hd2)  /dev/sda
(hd3)  /dev/sdb
```

Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der `device.map` manuell festzulegen. Sollten Sie Probleme beim Booten haben, kontrollieren Sie, ob die

Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht und ändern Sie sie notfalls mithilfe der GRUB-Shell (siehe Abschnitt 8.4.3) ab. Ist das Linux-System erst gebootet, können Sie die `device.map` mithilfe des YaST Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft abändern.

Nach manuellen Änderungen der `device.map` Datei, rufen Sie den folgenden Befehl auf, um GRUB neu zu installieren:

```
grub --batch --device-map=/boot/grub/device.map < /etc/grub.conf
```

8.4.3 Die Datei /etc/grub.conf

Die dritte wichtige Konfigurationsdatei von GRUB neben `menu.lst` und `device.map` ist `/etc/grub.conf`. Hier werden die Parameter und Optionen aufgeführt, die der Befehl `grub` benötigt, um den Bootloader korrekt zu installieren:

```
root (hd0,4)
install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

Die Bedeutung der einzelnen Einträge im Detail:

root (hd0,4) Mit diesem Befehl wird GRUB angewiesen, sich bei den folgenden Befehlen auf die erste logische Partition der ersten Festplatte zu beziehen, auf denen er seine Bootdateien findet.

install `parameter` Der Befehl `grub` soll mit dem `install`-Parameter gestartet werden. `stage1` als erste Stufe des Bootloaders soll in den MBR der ersten Festplatte installiert werden (`/grub/stage1 d (hd0)`). `stage2` soll in die Speicheradresse 0x8000 geladen werden (`/grub/stage2 0x8000`). Der letzte Eintrag `(hd0,4)/grub/menu.lst` weist `grub` an, wo die Menüdatei zu finden ist.

Die GRUB-Shell

GRUB existiert in zwei Versionen. Einmal als Bootloader und einmal als normales Linux-Programm unter `/usr/sbin/grub`. Dieses Programm wird als *GRUB-Shell* bezeichnet. Die Funktionalität, GRUB als Bootloader auf eine Festplatte oder Diskette zu installieren, ist direkt in GRUB integriert in Form der Kommandos `install` oder `setup`. Damit ist sie in der

GRUB-Shell verfügbar, wenn Linux geladen ist. Diese Befehle sind aber auch schon *während* des Bootvorgangs verfügbar, ohne dass Linux dazu laufen müsste. Dadurch vereinfacht sich die Rettung eines defekten Systems.

Nur wenn die GRUB-Shell als Linux-Programm läuft (aufzurufen mit `grub` wie beispielsweise unter Abschnitt 8.4.2 auf Seite 234 beschrieben), kommt der Zuordnungsalgorithmus von GRUB-Device und Linux-Device-Namen ins Spiel. Das Programm liest hierzu die Datei `device.map`. Mehr dazu im Abschnitt 8.4.2 auf Seite 234.

8.4.4 Bootpasswort setzen

GRUB unterstützt schon zum Bootzeitpunkt den Zugriff auf Dateisysteme, das heisst es können auch solche Dateien Ihres Linux-Systems eingesehen werden, zu denen Benutzer ohne Root-Rechte im einmal gestarteten System keinen Zugriff hätten. Durch Vergabe eines Passworts verhindern Sie solche Zugriffe. Einerseits können Sie lediglich den Dateisystemzugriff zur Bootzeit für Unbefugte sperren oder auch das Ausführen bestimmter Betriebsysteme für die Benutzer sperren.

Zur Vergabe eines Boot-Passworts gehen Sie als Benutzer `root` folgendermaßen vor:

- Geben Sie am Rootprompt `grub` ein.
- Verschlüsseln Sie in der GRUB-Shell das Passwort:

  ```
  grub> md5crypt
  Password: ****
  Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
  ```

- Fügen Sie den verschlüsselten Wert in den globalen Abschnitt der Datei `menu.lst` ein:

  ```
  gfxmenu (hd0,4)/message
  color white/blue black/light-gray
  default 0
  timeout 8
  password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
  ```

  Nun ist das Ausführen von GRUB-Befehlen am Bootprompt geschützt. Erst nach Eingabe von (p) und des Passworts wird diese Möglichkeit wieder freigegeben. Das Starten eines Betriebssystems aus dem Bootmenü heraus ist weiterhin für alle Benutzer möglich.

- Um zusätzlich das Starten einer oder mehrerer Betriebssysteme aus dem Bootmenü zu verhindern, ergänzen Sie in der Datei `menu.lst` den Eintrag `lock` für jeden Abschnitt, der nicht ohne Passworteingabe starten soll. Im Beispiel sähe dies so aus:

  ```
  title linux
  kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
  initrd (hd0,4)/initrd
  lock
  ```

  Nach einem Reboot des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

  ```
  Error 32: Must be authenticated
  ```

  Drücken Sie (Enter), um ins Menü zu gelangen und anschließend (p), um einen Prompt für das Passwort zu erhalten. Nach Eingabe des Passworts und (Enter) bootet das gewünschte Betriebssystem (in diesem Fall Linux).

Hinweis

Bootpasswort und Splashscreen

Verwenden Sie ein Bootpasswort für GRUB, steht Ihnen der gewohnte Splashscreen nicht zur Verfügung.

Hinweis

8.4.5 Mögliche Probleme und weitere Informationen

Hinweis

Bootprobleme mit GRUB

GRUB überprüft die Geometrie der angeschlossenen Festplatten erst beim Booten. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, so dass GRUB einen GRUB Geom Error meldet (siehe hierzu `http://portal.suse.com/sdb/de/2003/02/fhassel_geom-error.html`). In solchen Fällen verwenden Sie LILO oder aktualisieren ggf. das BIOS. Detaillierte Informationen zur Installation, Konfiguration und Wartung von LILO finden Sie in der Support-Datenbank `http://portal.suse.de/sdb/de/2004/01/lilo_overview.html`.

Hinweis

Auf der Webseite `http://www.gnu.org/software/grub/` finden Sie ausführliche Informationen zu GRUB in den Sprachen Deutsch und Englisch. Das Online-Handbuch existiert allerdings nur in Englisch.

Wenn texinfo auf dem Rechner installiert ist, können Sie sich in der Shell mit `info grub` die Info-Seiten zu GRUB anzeigen lassen. Suchen Sie auch in der Support-Datenbank `http://portal.suse.de/sdb/de/index.html` nach dem Stichwort GRUB, um Informationen zu speziellen Themen zu erhalten.

8.5 Booten mit LILO

Der Linux-Bootloader LILO ist für die Installation im MBR geeignet. LILO hat Zugriff auf beide im Real-Modus bekannten Festplatten und ist bereits von seiner Installation her in der Lage, alle benötigten Daten auf den „rohen“ Festplatten, ohne Informationen zur Partitionierung, zu finden. Deshalb lassen sich auch Betriebssysteme von der zweiten Festplatte booten. Die Einträge in der Partitionstabelle werden im Gegensatz zum DOS-Bootvorgang ignoriert.

Der Hauptunterschied zum DOS-Bootvorgang besteht in der Möglichkeit, beim Booten zwischen dem Laden verschiedener installierter Betriebssysteme wählen zu können. Nach dem Laden des MBR in den Speicher wird LILO gestartet; LILO bietet nun dem Benutzer die Auswahl aus einer Liste vorinstallierter Systeme an. Er kann beim Systemstart Bootsektoren von Partitionen laden, um ein Betriebssystem von dieser Partition zu starten, oder den Linux-Kernel laden und Linux starten. Zudem bietet er die wichtige Gelegenheit, dem Linux-Kernel eine Kommandozeile mitzugeben. Zu Sicherheitszwecken kann LILO ganz oder teilweise passwortgeschützt werden.

8.5.1 Grundlagen

Die LILO Startmaschinerie umfasst die folgenden Bestandteile:

- *LILO–Bootsektor* mit einem Anfangsstück („erste Stufe“) des LILO–Codes, das den eigentlichen LILO beim Systemstart aktiviert.
- LILO–Maschinencode, standardmäßig in `/boot/boot-menu.b`
- *Map-Datei* (`/boot/map`), in der LILO bei seiner Installation einträgt, wo die Linux–Kernel und sonstigen Daten, die er braucht, zu finden sind.

- optional: die *Message-Datei* `/boot/message`, die standardmäßig eine graphische LILO–Bootauswahl erzeugt.
- die verschiedenen Linux–Kernel und Bootsektoren, die LILO zum Starten anbieten soll.

Achtung

Zerstörung der Map-Datei durch Schreibzugriff

Jeder Schreibzugriff (auch durch Dateiverschiebung) auf einen dieser Bestandteile macht die Map-Datei ungültig und daher eine *Neuinstallation von LILO* erforderlich (siehe 8.5.4 auf Seite 244)! Dies betrifft vor allem den Wechsel zu einem neuen Linux-Kernel.

Achtung

Für den LILO–Bootsektor stehen folgende Installationsziele zur Auswahl:

Auf einer *Diskette* Dies ist die einfachste, aber auch langsamste Methode, mit LILO zu booten. Wählen Sie diese Methode, wenn Sie den bestehenden Bootsektor nicht überschreiben wollen.

Im *Bootsektor* einer primären Linux–Partition der ersten Festplatte Diese Variante lässt den MBR unberührt. Vor dem Booten muss diese Partition mit fdisk als aktiv markiert werden. Rufen Sie dazu als `root` `fdisk -s <Partition>` auf. fdisk fragt Sie nun nach einer Eingabe. `m` gibt Ihnen eine Liste der möglichen Eingaben und mit `a` können Sie die angegebene Partition startbar machen.

Im *Master Boot Record* Diese Variante bietet die größte Flexibilität. Insbesondere ist dies die einzige Möglichkeit, Linux von Festplatte aus zu booten, wenn sämtliche Linux-Partitionen auf der zweiten Festplatte liegen und auf der ersten keine erweiterte Partition zur Verfügung steht. Ein Veränderung des MBR birgt aber bei unsachgemäßer Installation auch gewisse Risiken.

Wenn Sie bisher einen *anderen Bootmanager* verwendet haben … … und ihn weiterverwenden wollen, gibt es, je nach dessen Fähigkeiten, noch weitere Möglichkeiten. Ein häufiger Fall: Sie haben eine primäre Linux-Partition auf der zweiten Platte, von der aus Sie Linux starten wollen. Ihr anderer Bootmanager wäre imstande, diese Partition über den Bootsektor zu starten. Dann können Sie diese Partition startbar machen, indem Sie LILO in deren Bootsektor installieren und sie dem anderen Bootmanager als startbar melden.

8.5.2 LILO-Konfiguration

Als flexibler Bootmanager bietet LILO zahlreiche Möglichkeiten, seine Konfiguration den individuellen Erfordernissen anzupassen. Die wichtigsten Optionen und ihre Bedeutung werden im Folgenden erläutert. Für eine umfassende Beschreibung sei auf [4] verwiesen.

Die Konfiguration von LILO wird in der Datei `/etc/lilo.conf` eingetragen. Es ist ratsam, die bei der letzten LILO–Installation verwendete Konfigurationsdatei sorgfältig aufzubewahren und vor jeder Änderung eine Sicherheitskopie herzustellen. Eine Änderung wird erst wirksam, indem Sie LILO mit der neuesten Fassung der Konfigurationsdatei neu installieren (Abschnitt 8.5.4 auf Seite 244)!

8.5.3 Der Aufbau der Datei lilo.conf

Die `/etc/lilo.conf` beginnt mit einem *globalen Abschnitt* (engl. *global options section*) mit allgemeinen Einstellungen, gefolgt von einem oder mehreren *System-Abschnitten* (engl. *image sections*) für die einzelnen Betriebssysteme, die LILO starten soll. Ein neuer Systemabschnitt wird jeweils eingeleitet durch eine Zeile mit der Option `image` oder `other`.

Die Reihenfolge der einzelnen Betriebssysteme in der `lilo.conf` ist nur insofern von Bedeutung, als das *zuerst* in der Liste aufgeführte System automatisch gebootet wird, wenn keine Benutzereingabe erfolgt – gegebenenfalls nach Ablauf einer vorkonfigurierten Wartezeit (s.u. die Optionen `delay` und `timeout`).

Datei 8.1 zeigt eine Beispielkonfiguration auf einem Rechner mit Linux und Windows. Beim Booten sollen zur Auswahl stehen: ein neuer Kernel (`/boot/vmlinuz`) und ein Linux-Kernel als Fallback (`/boot/vmlinuz.shipped`), sowie Windows auf `/dev/hda1` und das Programm Memtest86.

Beispiel 8.1: *Beispielkonfiguration in /etc/lilo.conf*

```
### LILO global section
boot    = /dev/hda           # LILO installation target: MBR
backup  = /boot/MBR.hda.990428  # backup file for the old MBR
                             # 1999-04-28
vga     = normal             # normal text mode (80x25 chars)
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32                        # Use BIOS to ignore
```

```
                              # 1024 cylinder limit
prompt
password = q99iwr4            # LILO password (example)
timeout = 80                  # Wait at prompt for 8 s before
                              # default is booted
message = /boot/message       # LILO's greeting

### LILO Linux section (default)
  image  = /boot/vmlinuz      # Default
  label  = linux
  root   = /dev/hda7          # Root partition for the kernel
  initrd = /boot/initrd

### LILO Linux section (fallback)
  image  = /boot/vmlinuz.shipped
  label  = Failsafe
  root   = /dev/hda7
  initrd = /boot/initrd.suse
  optional

### LILO other system section (Windows)
  other  = /dev/hda1          # Windows partition
  label  = windows

### LILO Memory Test
  image  = /boot/memtest.bin
  label  = memtest86
```

In `/etc/lilo.conf` ist alles von einem # bis zum Zeilenende ein Kommentar. Er wird ebenso wie Zwischenraum von LILO ignoriert und kann zur Verbesserung der Lesbarkeit verwendet werden. Zunächst werden die unbedingt notwendigen Einträge besprochen, die weiteren Optionen sind im anschließenden Abschnitt 8.5.3 auf der vorherigen Seite beschrieben.

- **Globaler Abschnitt** (Parameterteil)
  - `boot=bootdevice`
    Device auf dessen erstem Sektor der LILO–Bootsektor installiert werden soll (das Installationsziel). `bootdevice` kann sein: ein Diskettenlaufwerk (`/dev/fd0`), eine Partition (z.B. `/dev/hdb3`), oder eine ganze Platte (z.B. `/dev/hda`): letzteres bedeutet die Installation im MBR. Voreinstellung: Fehlt diese

Angabe, wird LILO auf der gegenwärtigen Linux–Rootpartition installiert.

- `lba32`

  Diese Option umgeht die 1024–Zylinder–Grenze von LILO. Dies funktioniert natürlich nur, wenn das BIOS Ihres Rechners dies auch unterstützt.

- `prompt`

  Erzwingt das Erscheinen der LILO–Eingabeaufforderung (Prompt). Die Voreinstellung ist: kein Prompt! (Vgl. Abschnitt 8.5.3 auf Seite 240, Option `delay`.)

  Empfohlen, sobald LILO mehr als nur ein System starten soll. Zusammen damit sollte auch die `timeout`-Option gesetzt werden, damit ein automatischer Reboot möglich ist, wenn keine Eingabe erfolgt.

- `timeout=zehntelsekunden`

  Setzt eine Auszeit für die Wahl des zu startenden Systems und ermöglicht dadurch das automatische Booten, wenn nicht rechtzeitig eine Auswahl erfolgt. `zehntelsekunden` ist dabei die verbleibende Zeit in Zehntelsekunden für eine Eingabe. Durch Drücken von (Shift) wird diese Funktion außer Kraft gesetzt und der Rechner wartet auf Ihre Eingabe. Die Voreinstellung ist `80`.

- **Linux-Abschnitt**

  - `image=kernelimage`

    Hier muss der Name des zu bootenden Kernel-Images stehen. Dies wird in der Regel `/boot/vmlinuz` sein.

  - `label=<name>`

    Innerhalb der `/etc/lilo.conf` eindeutiger, aber sonst frei wählbarer Name für das System (z.B. `Linux`). Maximale Länge 15 Zeichen: möglichst nur Buchstaben, Ziffern und Unterstrich – keine Leerzeichen, Sonderzeichen wie deutsche Umlaute u.Ä. Die genauen Regeln für erlaubte Zeichen finden Sie in Abschnitt [4]. Die Voreinstellung ist Dateiname des Kernel-Images (zum Beispiel `/boot/vmlinuz`).

    Unter diesem Namen wählen Sie beim Systemstart das gewünschte Betriebssystem aus. Bei mehreren Systemen empfiehlt es sich, eine nähere Beschreibung der Namen und Systeme in einer message–Datei (siehe Abschnitt 8.5.3 auf Seite 240, Option `message`) bereitzustellen.

- ▷ `root=<rootdevice<`
  Damit gibt LILO dem Kernel die Rootpartition (z.B. `/dev/hda2`) des Linux-Systems an. Zur Sicherheit empfohlen! Wird diese Option weggelassen, nimmt der Kernel die in ihm selbst eingetragene Rootpartition `<kernelimage>`.
- ▷ `append=<parameter>`
  Möchten Sie LILO nachträglich weitere Bootoptionen für den Kernel übergeben, fügen Sie der bestehenden `lilo.conf` eine mit `append` beginnende Zeile hinzu und geben nach dem = Zeichen die entsprechenden Parameter durch Leerzeichen getrennt und in Anführungsstrichen ein. Nach dieser Änderung muss LILO als Benutzer `root` mit `lilo` neu installiert werden, damit beim nächsten Booten Ihre Änderungen übernommen werden.

- **Linux-Abschnitt** (Linux – Safe Settings)
  Auch wenn ein eigener Kernel installiert wurde, ist es immer möglich, auf diesen Kernel zurückzugreifen und das System zu starten.
  - ▷ `optional`
    Sollte `/boot/vmlinuz.shipped` gelöscht werden (*nicht* empfehlenswert!), wird bei der LILO-Installation dieser Abschnitt ohne Fehlermeldung übergangen.

- **Anderes System**
  - ▷ `other=<partition>`
    Mit `other` werden LILO Startpartitionen anderer Systeme zum Booten bekannt gemacht (z.B. `/dev/hda1`).
  - ▷ `label=name`
    Wählen Sie hier einen Name für dieses System. Die Voreinstellung – der bloße Device–Name der Partition – ist beim Booten nicht sehr aussagekräftig.

- **Memory Test**
  Hier ist nur das Programm zum Testen des Speichers eingetragen.

Im diesem Abschnitt wurden nur die in `/etc/lilo.conf` minimal nötigen Einträge besprochen. Weitere nützliche Einstellungen entnehmen Sie bitte der Manual-Page von `lilo.conf`, die Sie mit dem Befehl `man lilo.conf` erhalten.

8.5.4 Installation und Deinstallation von LILO

Achtung

Booten von anderen Betriebssystemen

Vergewissern Sie sich vor der Installation von LILO *auf jeden Fall*, dass Sie eventuell vorhandene andere Betriebssysteme von Diskette booten können (funktioniert nicht bei Windows XP/2000/NT)! Vor allem fdisk muss zur Verfügung stehen. SUSE LINUX kann gegebenenfalls auch von der Installations-CD bzw. -DVD gebootet werden.

Achtung

Installation nach Änderung der Konfiguration

Wenn sich an den LILO–Komponenten etwas geändert hat oder wenn Sie Ihre Konfiguration in `/etc/lilo.conf` modifiziert haben, müssen Sie LILO neu installieren. Dies geschieht durch einfachen Aufruf des sog. *Map-Installers* als Benutzer `root`: `/sbin/lilo`.

LILO legt daraufhin ein Backup des Ziel–(Boot-)Sektors an, schreibt seine „erste Stufe“ in diesen Sektor und erzeugt eine neue Map–Datei. LILO meldet nacheinander die installierten Systeme – z.B. im Fall unser obigen Beispielkonfiguration:

```
Added linux * Added suse Added windows Added memtest86
```

Nach abgeschlossener Installation kann der Rechner neu gestartet werden (als Benutzer `root`): `shutdown -r now`.

Nachdem das BIOS seinen Systemtest ausgeführt hat, meldet sich LILO mit seiner Eingabeaufforderung, an der Sie LILO Parameter für den Kernel übergeben und das gewünschte Bootimage auswählen können. Mit Tab lassen sich die Bezeichnungen der installierten Konfigurationen auflisten.

8.6 Bootloader-Konfiguration mit YaST

Die Bootloader-Konfiguration wird durch das YaST-Modul stark vereinfacht, allerdings sollten Sie sich nicht daran versuchen, ohne das Konzept dahinter verstanden zu haben. Die folgenden Erklärungen beziehen sich primär auf den Standard-Bootloader GRUB.

Hinweis

Das Ändern des Boot-Modus im laufenden System ist nur für Experten zu empfehlen.

Hinweis

Rufen Sie im YaST Kontrollzentrum unter ‘System’ das Modul ‘Bootloader-Konfiguration’ auf. Sie sehen die aktuelle Bootloader-Konfiguration Ihres Systems und können diese nun verändern (siehe Abb. 8.1).

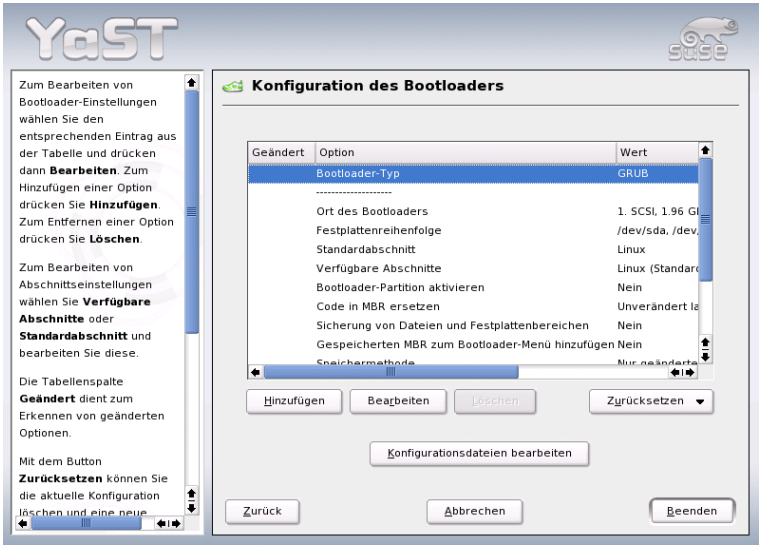

Abbildung 8.1: *Bootloader-Konfiguration mit YaST*

8.6.1 Das Hauptfenster

Das weiß unterlegte Konfigurationsfeld gliedert sich in drei Spalten, links unter ‘Geändert’ werden die veränderten Optionen markiert, die in der mittleren Spalte aufgeführt sind. Die aktuellen Werte dazu finden Sie in der rechten Spalte. Um nun eine neue Option hinzuzufügen, klicken Sie auf den Button ‘Hinzufügen’. Wenn Sie dagegen nur den Wert einer Option ändern wollen, wählen Sie diese durch Mausklick aus und klicken dann auf

'Bearbeiten'. Wollen Sie eine bestehende Option nicht verwenden, wählen Sie sie aus und klicken auf 'Löschen'.

Rechts unter dem Konfigurationsfenster finden Sie eine Combobox 'Zurücksetzen' mit folgenden Optionen:

Neue Konfiguration vorschlagen Ein neuer Konfigurationsvorschlag wird erstellt. Wenn dabei auf anderen Partitionen eine ältere Linux-Version oder ein anderes Betriebssystem gefunden werden, werden diese in das Bootmenü integriert. Sie können dann wählen, ob Linux direkt gebootet wird oder dessen alter Bootloader. Im letzteren Fall gelangen Sie dann beim Booten in ein zweites Bootmenü.

Starten von Scratch Sie erstellen selbst die gesamte Konfiguration ohne Unterstützung durch Vorschläge.

Konfiguration neu von Festplatte einlesen
Wenn Sie schon einige Veränderungen vorgenommen haben und mit dem Ergebnis nicht zufrieden sind, können Sie hier die aktuell gespeicherte Konfiguration neu einlesen. Als Ausgangsbasis haben Sie dann wieder den Stand, der im System gespeichert ist.

Vorschlagen und mit vorhandene GRUB-Menüs mergen
Falls ein anderes Betriebssystem und eine ältere Linux-Version in anderen Partitionen installiert sind, wird das Menü aufgebaut aus einem Eintrag für das neue SUSE LINUX, einem Eintrag für das andere System sowie allen Einträgen aus dem alten Bootloader-Menü. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Bei Verwendung von LILO besteht diese Möglichkeit nicht.

MBR von Festplatte wiederherstellen
Hier wird der auf Festplatte gespeicherte MBR wieder zurückgeschrieben.

Unterhalb dieser Combobox finden Sie den Button 'Konfigurationsdateien bearbeiten', über den Sie direkt die relevanten Konfigurationsdateien in einem Editor bearbeiten können. Über das Auswahlfeld laden Sie die gewünschte Datei und können diese direkt ändern. Bei Klick auf 'OK' werden Ihre Änderungen gespeichert. Mit 'Abbrechen' verlassen Sie die Bootloader-Konfiguration und 'Zurück' bringt Sie wieder zum Hauptfenster.

Achtung

Beachten Sie, dass die Reihenfolge der Optionen bzw. Befehle bei GRUB eine wichtige Rolle spielt. Richten Sie sich nach der vorgegebenen Reihenfolge, da der Rechner sonst eventuell nicht startet.

Achtung

8.6.2 Optionen der Bootloader-Konfiguration

Für weniger erfahrene Benutzer ist die YaST-geführte Konfiguration wesentlich einfacher als das direkte Editieren der Dateien. Selektieren Sie mit der Maus eine Option und klicken dann auf 'Bearbeiten', erscheint ein Dialog, in dem Sie individuelle Anpassungen vornehmen können. Durch Klick auf 'OK' bestätigen Sie die Änderungen und gelangen zurück zum Hauptdialog, wo Sie weitere Optionen bearbeiten können. Diese Optionen sind je nach Bootloader unterschiedlich. Im Folgenden stellen wir Ihnen kurz einige wichtige für GRUB vor:

Bootloader-Typ Über diese Option können Sie zwischen GRUB und LILO umschalten. Sie gelangen dann zu einem weiteren Dialog, in dem Sie die Art des Wechsels spezifizieren. Sie können die aktuelle GRUB-Konfiguration in eine ähnliche LILO-Konfiguration umwandeln lassen, wobei Informationen verloren gehen können, wenn es keine äquivalenten Optionen gibt. Außerdem können Sie die Konfiguration völlig neu erstellen oder sich einen neuen Vorschlag erstellen lassen, den Sie dann gegebenenfalls weiter bearbeiten.

Wenn Sie die Bootloader-Konfiguration im laufenden System aufrufen, können Sie weiterhin die Konfiguration von der Festplatte einlesen lassen. Falls Sie sich entscheiden sollten, doch wieder zum vorher eingestellten Bootloader zurückzuwechseln, können Sie über die letzte Option dessen Konfiguration wieder laden. Allerdings ist dies nur möglich, solange Sie das Bootloader-Modul nicht verlassen.

Ort des Bootloaders In diesem Dialog wird bestimmt, wohin der Bootloader installiert werden soll. Im Master Boot Record (MBR), im Bootsektor der Boot-Partition (falls vorhanden), im Bootsektor der root-Partition oder auf Diskette. Über die Option 'Andere' können Sie das Installationsziel frei wählen. Bitte beachten Sie dazu die Informationen zu GRUB oder LILO im *Installation und Administration*.

Festplatten-Reihenfolge Wenn Sie zwei oder mehr Festplatten in Ihrem Rechner eingebaut haben, geben Sie hier die Reihenfolge entsprechend den BIOS-Einstellungen des Rechners an.

Standardabschnitt Mit dieser Option legen Sie fest, welcher Kernel oder welches andere Betriebssystem als Standard geladen werden soll, wenn Sie im Bootmenü keine Wahl treffen. Dieses Betriebssystem wird nach Ablauf der Wartefrist automatisch gebootet. In diesem Menü gelangen Sie über den Button 'Bearbeiten' zur Übersicht aller Bootmenü-Einträge. Wählen Sie aus der Liste den gewünschten Eintrag aus und aktivieren Sie dann 'Als Standard festlegen'. Sie können an dieser Stelle auch einen beliebigen Eintrag durch Klick auf 'Ändern' editieren.

Verfügbare Abschnitte Im Hauptfenster sehen Sie bei dieser Option, welche Menü-Einträge es gibt. Wenn Sie diese Option auswählen und auf 'Ändern' klicken, gelangen Sie zum selben Dialog wie bei 'Standard-Eintrag'.

Bootloader-Partition aktivieren Mit dieser Option aktivieren Sie die Partition, in deren Bootsektor der Bootloader installiert wurde unabhängig davon, auf welcher Partition das Verzeichnis `/boot` oder `/` (root) mit den Bootloader-Dateien liegt.

Code im MBR ersetzen Wenn Sie die Lage des Bootloaders verändern, können Sie hier entscheiden, ob der MBR überschrieben werden soll.

Sicherung von Dateien und Festplattenbereichen
Die geänderten Festplattenbereiche werden gesichert.

Gespeicherten MBR zum Bootloader-Menü hinzufügen
Fügen Sie den gespeicherten MBR zum Bootloadermenü hinzu.

Im untersten Abschnitt ist die 'Timeout'-Option interessant, mit der Sie festlegen können, wie viele Sekunden der Bootloader auf Eingaben wartet, bis er das Standard-System bootet. An dieser Stelle können Sie noch eine Reihe weiterer Optionen über den 'Hinzufügen'-Button ergänzen. Die sinnvolle Nutzung dieser Optionen erfordert in der Regel jedoch ein tiefes Verständnis der Hintergründe und wird deshalb hier nicht weiter erläutert. Lesen Sie dazu bitte die entsprechenden Kapitel im *Installation und Administration* sowie in den Manual-Pages von GRUB und LILO (Befehle: `man grub, man lilo, man lilo.conf`). Zu GRUB finden Sie außerdem ein ausführliches Online-Handbuch auf der Webseite: `http://www.gnu.org/software/grub/`.

8.7 Linux-Bootloader entfernen

Es stehen zwei Methoden zur Auswahl, um den Linux-Bootloader zu deinstallieren:

- Spielen Sie das Backup des ursprünglichen MBRs mittels des YaST-Bootloader-Moduls wieder ein. YaST erstellt dieses Backup automatisch. Eine Beschreibung des YaST Bootloader-Moduls finden Sie im Installationsteil des *Benutzerhandbuchs*.
- Installieren Sie einen anderen Bootloader oder stellen Sie den DOS/Windows-MBR wieder her.

Achtung

Ungültige Backups von Bootsektoren

Ein Backup des Bootsektors wird ungültig, wenn die betreffende Partition ein neues Dateisystem erhalten hat. Die Partitionstabelle in einem MBR-Backup wird ungültig, wenn die betreffende Festplatte zwischenzeitlich anders partitioniert worden ist. Solche Backups sind „Zeitbomben“: am Besten sofort in `/boot/backup.mbr`löschen!

Achtung

8.7.1 MBR wiederherstellen (DOS/Win9x/ME)

Einen DOS- oder Windows-MBR stellt man mit dem MS-DOS-Befehl `fdisk /MBR` (verfügbar ab DOS Version 5.0) wieder her. Oder unter OS/2 mit dem Befehl: `fdisk /newmbr`.

Diese Befehle schreiben nur die 446 ersten Bytes (den Boot-Code) in den MBR zurück und lassen die gegenwärtige Partitionstabelle unangetastet. Außer, wenn der MBR (siehe 8.1.1 auf Seite 224) wegen einer falschen „magischen Zahl“ als im ganzen ungültig behandelt wird: dann wird die Partitionstabelle genullt. *Nicht vergessen:* Mit fdisk die von jetzt an gewünschte Startpartition wieder als *aktiv bootable* kennzeichnen; die MBR–Routinen von DOS, Windows, OS/2 brauchen das.

8.7.2 MBR wiederherstellen (Windows XP)

Booten Sie von der Windows XP CD, drücken Sie im Setup die Taste Ⓡ, um die Wiederherstellungskonsole zu starten. Wählen Sie aus der Liste Ihre Windows XP Installation aus und geben Sie das Administratorpasswort ein. Geben Sie in die Eingabeaufforderung den Befehl `FIXMBR` ein und bestätigen Sie die Sicherheitsabfrage mit `j`. Mit `exit` können Sie den Computer anschließend neu starten.

8.7.3 MBR wiederherstellen (Windows 2000)

Booten Sie von der Windows 2000 CD, drücken Sie im Setup die Taste Ⓡ, sowie im darauf folgenden Menü die Taste Ⓚ, um die Wiederherstellungskonsole zu starten. Wählen Sie aus der Liste Ihre Windows 2000 Installation aus und geben Sie das Administratorpasswort ein. Geben Sie in die Eingabeaufforderung den Befehl `FIXMBR` ein und bestätigen Sie die Sicherheitsabfrage mit `j`. Mit `exit` können Sie den Computer anschließend neu starten.

8.8 Für alle Fälle: Boot-CD erstellen

Falls Sie Probleme haben, Ihr installiertes System über einen Bootmanager zu booten oder Lilo oder Grub nicht in den MBR Ihrer Festplatte, noch auf eine Diskette installieren wollen oder können, ist es auch möglich, eine bootfähige CD zu erstellen, auf die Sie die Linux Startdateien brennen. Voraussetzung hierfür ist natürlich, dass ein Brenner in Ihrem System vorhanden und eingerichtet ist.

8.8.1 Boot-CD mit ISOLINUX

Um eine bootfähige CD zu erstellen, ist es am einfachsten, den Bootmanager Isolinux zu verwenden. Auch die SuSE Installations-CDs werden übrigens per Verwendung von Isolinux bootfähig gemacht.

- Booten Sie Ihr installiertes System zunächst auf folgendem Umweg: Legen Sie die Installations-CD oder -DVD in Ihr Laufwerk und booten Sie von dieser wie bei der Installation. Wählen Sie dann im Bootmenü die Option ‘Installation’ aus und im nächsten Menu den Punkt ‘Installiertes System booten’. Dabei wird die root-Partition automatisch erkannt, sodass von dieser das System gebootet werden kann.

- Installieren Sie mit Hilfe von YaST das `syslinux`.
- Öffnen Sie eine Root-Shell. Mit Hilfe der folgenden Aufrufe wird für die Boot-CD ein temporäres Verzeichnis erstellt und die zum Booten des Linux Systems notwendigen Dateien (der Bootloader Isolinux sowie der Kernel und die Initrd) hineinkopiert.

```
mkdir /tmp/CDroot
cp /usr/share/syslinux/isolinux.bin /tmp/CDroot/
cp /boot/vmlinuz /tmp/CDroot/linux
cp /boot/initrd /tmp/CDroot
```

- Erstellen Sie mit einem Editor die Bootloader-Konfigurationsdatei `/tmp/CDroot/isolinux.cfg`. Tragen Sie folgenden Inhalt ein:

```
DEFAULT linux
LABEL linux
  KERNEL linux
  APPEND initrd=initrd root=/dev/hdXY [bootparameter]
```

  Für den Parameter `root=/dev/hdXY` tragen Sie bitte Ihre root-Partition ein. Wenn Sie sich nicht sicher sind, welche Partitionsbezeichnung diese hat, schauen Sie einfach in der Datei `/etc/fstab` nach. Für den Wert `[bootparameter]` können Sie zusätzliche Optionen eingeben, die beim Booten verwendet werden sollen. Die Konfigurationsdatei könnte zum Beispiel folgendermaßen aussehen:

```
DEFAULT linux
LABEL linux
  KERNEL linux
  APPEND initrd=initrd root=/dev/hda7 hdd=ide-scsi
```

- Anschließend wird mit folgendem Aufruf aus den Dateien ein ISO9660-Dateisystem für die CD erstellt (schreiben Sie das folgende Kommando in eine Zeile):

```
mkisofs -o /tmp/bootcd.iso -b isolinux.bin -c boot.cat
  -no-emul-boot -boot-load-size 4
  -boot-info-table /tmp/CDroot
```

- Brennen Sie die Datei `/tmp/bootcd.iso` auf CD, entweder mit graphischen Brennprogrammen wie K3b oder einfach von der Kommandozeile: `cdrecord -v -eject speed=2 dev=0,0,0 /tmp/bootcd.iso`.

  Evtl. muss der Parameter `dev=0,0,0` an die SCSI-ID des Brenners angepasst werden (diese erfahren Sie durch Eingabe des Aufrufs `cdrecord -scanbus`, vergleiche auch die Manualpage mit `man cdrecord`).

- Testen Sie die Boot-CD! Rebooten Sie dazu den Computer und überprüfen Sie ob Ihr Linux-System korrekt von der CD gestartet wird.

8.9 S/390, zSeries: Der Bootloader ZIPL

Sobald SUSE LINUX auf den DASDs installiert wurde, müssen Sie die notwendigen Informationen für den IPL erstellen. Diese Informationen schliessen den Speicherort des Kernelimages und die Parameterzeile ein. Benutzen Sie hierzu das Programm ZIPL, das diese Informationen entweder von der Kommandozeile übernimmt oder aus einer Konfiguartionsdatei liest.

8.9.1 Verwendung

In Verbindung mit Kernel Version 2.6.x

ZIPLs Syntax ist wie folgt:

```
zipl [options] [configuration]

Options:
 -h or --help     prints this information
 -c <CONFIG-FILE> or --config=<CONFIG-FILE>
      <CONFIG-FILE> specifies the config file to be used.
      This option overrides the environment variable
      ZIPLCONF.
```

Die folgenden Optionen übersteuern die Einstellungen der Konfigurationsdatei:

`-t <DIRECTORY>` oder `--target=<DIRECTORY>`
⟨*DIRECTORY*⟩ legt das Zielverzeichnis fest in das ZIPL eine Dateien für den ipl Prozess ablegt

`-i <IMAGE[,ADDRESS]>` oder `--image=<IMAGE[,ADDRESS]>`
⟨*IMAGE*⟩ gibt den Dateinamen des zu bootenden Kernelimages an, ⟨*ADDRESS*⟩ legt die Ladeadresse des Images im Hauptspeicher fest

`-r <RAMDISK[,ADDRESS]>` oder `--ramdisk=<RAMDISK[,ADDRESS]>`
⟨*RAMDISK*⟩ gibt den Dateinamen der Ramdisk fest, die geladen werden soll ⟨*ADDRESS*⟩ legt die Ladeadresse der Ramdisk im Haupsteicher fest

`-p <PARMFILE[,ADDRESS]>` oder `--parmfile=<PARMFILE[,ADDRESS]>`
⟨*PARMFILE*⟩ gibt den Dateinamen der Parameterdatei an ⟨*ADDRESS*⟩ legt die Ladeadresse der Parameterdatei im Hauptspeicher fest

`-d <PARTITION>` oder `--dumpto <PARTITION>`
⟨*PARTITION*⟩ gibt die Gerätedatei an, auf der ein Speicherabzug erstellt werden soll. Beispiel: `/dev/dasdb1` oder `/devfs/dasd/0192/part1`

Beachten Sie, dass ⟨*ARG*⟩ ein notwendiges Argument darstellt, während ⟨*[ARG]*⟩ optionale Parameter enthält.

Der Befehl `zipl` liest die Konfigurationsdatei `/etc/zipl.conf` und benutzt die Parameter aus dieser Datei.

Die ZIPL Konfigurationsdatei

Die Konfigurationsdatei des ZIPL Bootloaders befindet sich unter `/etc/zipl.conf`.

Beispiel 8.2 zeigt Ihnen eine `zipl.conf` Datei. Sie ist in mehrere Sektionen aufgeteilt. Sie können hier mehrere Wege zum IPL des Linux Systems definieren.

Beispiel 8.2: `/etc/zipl.conf`

```
[defaultboot]
    default = ipl

[ipl]
    target = /boot/zipl
    image = /boot/image
    ramdisk = /boot/initrd
    parameters = "root=/dev/dasda2 term=dumb"
```

```
[dumpdasd]
    target = /boot/zipl
    dumpto = /dev/dasd??

[dumptape]
    target = /boot/zipl
    dumpto = /dev/rtibm0
```

Die Sektion `[defaultboot]` legt fest, welche Sektion aufgerufen wird, wenn ZIPL ohne Angabe weiterer Parameter gestartet wird.

Die Parameterzeile `parameters=...` gibt an, welche Kommandos während des Bootens an den Kernel übergeben werden.

Hinweis

Hinzufügen oder Herausnehmen von DASDs

Das Hinzufügen bzw. Herausnehmen eines oder mehrerer DASDs wird nun über YaST geregelt und sollte nicht mehr über die Datei `/etc/zipl.conf` erfolgen (wie es in früheren System der Fall war).

Hinweis

Der Linux Kernel

Der Kernel verwaltet die Hardware jedes Linux Systems und stellt diese den verschiedensten Prozessen zur Verfügung. Auf den folgenden Seiten wird man nicht lernen, wie man Kernel-„Hacker“ wird, aber man erfährt, wie man ein Kernel-Update durchführt, und wird in die Lage versetzt, sich einen selbstkonfigurierten Kernel zu kompilieren und zu installieren. Wenn Sie so vorgehen, wie in diesem Kapitel beschrieben, bleibt der bisherige Kernel funktionsfähig und kann jederzeit auf Wunsch gebootet werden.

9.1 Kernel-Update 256
9.2 Die Kernelquellen 257
9.3 Konfiguration des Kernels 257
9.4 Kernel-Module 259
9.5 Einstellungen bei der Kernelkonfiguration 262
9.6 Übersetzen des Kernels 262
9.7 Kernel installieren 263
9.8 Festplatte nach der Übersetzung aufräumen 265

Der Kernel, der bei der Installation im `/boot/`-Verzeichnis abgelegt wird, ist so konfiguriert, dass er ein möglichst breites Spektrum von Hardware unterstützt. Es ist meist *nicht erforderlich*, einen eigenen Kernel zu generieren, außer Sie wollen „experimentelle“ Features oder Treiber ausprobieren.

Zum Erzeugen eines neuen Kernels existieren bereits `Makefiles`, mit deren Hilfe der Ablauf fast völlig automatisiert ist. Lediglich die Auswahl der vom Kernel zu unterstützenden Hardware und Features muss interaktiv durchlaufen werden. Da Sie Ihr Computer-System ziemlich gut kennen müssen, um eine funktionierende Auswahl zu treffen, empfehlen wir – wenigstens für die ersten Versuche – eine bestehende und funktionierende Konfigurationsdatei abzuändern und damit die Gefahr falscher Einstellungen zu vermindern.

9.1 Kernel-Update

Um einen SUSE Update-Kernel zu installieren, laden Sie das Update-Paket vom SUSE FTP-Server oder einem Mirror wie zum Beispiel: `ftp://ftp.gwdg.de/pub/linux/suse/` herunter. Wenn Sie nicht wissen, welcher Kernel aktuell bei Ihnen läuft, so können Sie zum einen den version-String ansehen: `cat /proc/version`.

Sie können außerdem prüfen, zu welchem Paket der Kernel `/boot/vmlinuz` gehört: `rpm -qf /boot/vmlinuz`.

Vor der Installation sollten Sie den ursprünglichen Kernel und die dazugehörige `initrd` sichern. Geben Sie dazu als `root` die folgenden beiden Befehle ein:

```
cp /boot/vmlinuz /boot/vmlinuz.old
cp /boot/initrd /boot/initrd.old
```

Installieren Sie nun das neue Paket mit dem Befehl `rpm -Uvh <Paketname>`. Setzen Sie dabei die entsprechende Versionsnummer ein.

Seit SUSE LINUX 7.3 wird reiserfs als Standardfilesystem verwendet, was den Einsatz einer „initial ramdisk“ voraussetzt. Diese wird mit dem Befehl `mk_initrd` neu geschrieben. Bei aktuellen SUSE LINUX Versionen geschieht dies automatisch bei der Installation des Kernels.

Um gegebenenfalls den alten Kernel booten zu können, muss der Bootloader entsprechend konfiguriert werden. Genaue Informationen dazu finden Sie im Kapitel 8 auf Seite 223.

Wenn Sie den Original-Kernel von den SUSE LINUX CDs installieren möchten, gehen Sie ähnlich vor. Auf CD 1 oder der DVD finden Sie im Verzeichnis `boot/` den Standard Kernel als rpm-Paket. Installieren Sie diesen wie oben beschrieben. Falls Sie eine Fehlermeldung erhalten, dass bereits ein neueres Paket installiert ist, müssen Sie die Option `--force` beim rpm-Kommando zusätzlich angeben.

9.2 Die Kernelquellen

Um einen Kernel bauen zu können, müssen die Kernelquellen (Paket `kernel-source`) installiert werden. Andere erforderliche Pakete wie der C-Compiler (Paket `gcc`), die GNU Binutils (Paket `binutils`) und die Include-Dateien für den C-Compiler (Paket `glibc-devel`) werden dabei automatisch mit ausgewählt.

Die Kernelquellen befinden sich nach der Installation im Verzeichnis `/usr/src/linux-<kernel-version>/`. Sollten Sie vorhaben, mit dem Kernel zu experimentieren und verschiedene Versionen des Kernels gleichzeitig auf der Platte zu halten, so bietet es sich an, die einzelnen Versionen in verschiedene Verzeichnisse zu entpacken und die augenblicklich relevanten Quellen über einen Link anzusprechen, da es Software-Pakete gibt, die die Kernelquellen unter `/usr/src/linux` erwarten. Diese Form der Installation wird von YaST automatisch vorgenommen.

9.3 Konfiguration des Kernels

Die Konfiguration des aktuell laufenden Kernel ist in der Datei `/proc/config.gz` gespeichert. Um diese Konfiguration nach Ihren Wünschen anzupassen, wechseln Sie als Benutzer `root` in das Verzeichnis `/usr/src/linux/` und führen folgende Befehle aus:

```
zcat /proc/config.gz > .config
make oldconfig
```

Der Befehl `make oldconfig` verwendet die Datei `/usr/src/linux/.config` als Vorlage zur aktuellen Kernelkonfiguration. Wenn bei Ihren aktuellen Kernel-Sourcen neue Optionen hinzugekommen sind, so werden diese jetzt abgefragt.

Wenn die Datei `.config` fehlt, dann wird eine „default“ Konfiguration verwendet, die in den Kernel-Sourcen enthalten ist.

9.3.1 Kommandozeilenkonfiguration

Um den Kernel zu konfigurieren, wechseln Sie nach `/usr/src/linux` und geben den Befehl `make config` ein.

Sie werden nach einer Reihe von Systemfähigkeiten gefragt, die der Kernel unterstützen soll. Bei der Beantwortung der Fragen gibt es normalerweise zwei oder drei Möglichkeiten: Entweder einfaches (y) und (n), oder eine der drei Möglichkeiten (y) (*yes*), (n) (*no*) und (m) (*module*). (m) bedeutet hierbei, dass der entsprechende Treiber nicht fest zum Kernel hinzugebunden wird, sondern vielmehr als Modul übersetzt wird, das zur Laufzeit zum Kernel hinzugeladen werden kann. Sämtliche Treiber, die zum Booten des Systems unbedingt benötigt werden, müssen fest zum Kernel hinzugebunden werden; in diesen Fällen also (y) wählen. Mit (Enter) bestätigen Sie die Vorauswahl, die aus der Datei `.config` eingelesen wird. Wenn Sie bei einer Frage eine andere Taste drücken, erhalten Sie einen kurzen Hilfetext zu der jeweiligen Option angezeigt.

9.3.2 Konfiguration im Textmodus

Angenehmer lässt sich die Konfiguration des Kernels mit „menuconfig“ durchführen; gegebenenfalls müssen Sie dazu das `ncurses-devel` mit YaST nachinstallieren. Starten Sie die Kernel-Konfiguration mit dem Befehl `make menuconfig`.

Bei einer geringfügigen Änderung der Konfiguration müssen Sie sich hier nicht durch alle Fragen „durchtasten“, sondern können über das Menü direkt bestimmte Bereiche wählen. Die Voreinstellungen werden der Datei `.config` entnommen. Um eine andere Konfiguration zu laden, wählen Sie den Menüpunkt ‘Load an Alternate Configuration File’ und geben den Dateinamen an.

9.3.3 Konfiguration unter dem X Window System

Haben Sie das X Window System (Paket `xf86`) sowie Tcl/Tk (Paket `tcl` und `tk`) installiert, können Sie die Konfiguration alternativ durch den Befehl `make xconfig` vornehmen.

Sie haben dann eine grafische Oberfläche, die das Konfigurieren komfortabler macht. Dazu müssen Sie das X Window System aber als Benutzer `root` gestartet haben oder in der Shell zuerst als normaler Benutzer `xhost +` eingeben, um `root` Zugriff auf das Display zu gewähren. Die Voreinstellungen werden aus der Datei `.config` ausgelesen. Beachten Sie,

daß die Konfiguration über `make xconfig` nicht so gut gepflegt ist, wie die anderen Konfigurationsmöglichkeiten. Sie sollten daher nach dieser Konfigurationmethode immer noch ein `make oldconfig` ausführen.

9.4 Kernel-Module

Es gibt eine große Vielfalt an PC-Hardware-Komponenten. Um diese Hardware richtig benutzen zu können, braucht man einen „Treiber“, über den das Betriebssystem (bei Linux der „Kernel“) die Hardware richtig ansprechen kann. Generell gibt es zwei Mechanismen, Treiber in den Kernel zu integrieren:

- Die Treiber können fest in den Kernel einkompiliert sein. Solche Kernel „aus einem Stück“ bezeichnen wir in diesem Buch auch als *monolithische* Kernel. Manche Treiber können nur in dieser Form verwendet werden.
- Die Treiber können erst bei Bedarf in den Kernel geladen werden, der in diesem Fall als *modularisierter* Kernel bezeichnet wird. Das hat den Vorteil, dass wirklich nur die benötigten Treiber geladen sind und dass der Kernel keinen unnötigen Ballast enthält.

Welche Treiber fest zum Kernel gebunden und welche als Module realisiert werden, wird bei der Konfiguration des Kernels festgelegt. Alle Kernel-Komponenten, die nicht zwingend während des Bootvorgangs benötigt werden, sollten als Module realisiert werden. So wird sichergestellt, dass der Kernel nicht zu groß wird und dass der Kernel ohne Schwierigkeiten vom BIOS und einem beliebigen Bootloader geladen werden kann. Der Festplatten-Treiber, Unterstützung für `ext2` und ähnliche Dinge sind also im Regelfall direkt in den Kernel hineinzukompilieren, Unterstützung für `isofs`, `msdos` oder `sound` sollten in jedem Fall als Module kompiliert werden.

Die Kernelmodule werden in dem Verzeichnis `/lib/modules/<Version>/` abgelegt, wobei `Version` der momentanen Version des Kernels entspricht.

9.4.1 Erkennung der akutellen Hardware mit hwinfo

Unter SUSE LINUX steht Ihnen das Programm hwinfo zur Verfügung, mit der die aktuelle Hardware des Rechners erkannt werden kann, und die ver-

fügbaren Treiber zugeordnet werden. Eine kurze Hilfestellung zu diesem Programm bekommen Sie mit dem Befehl `hwinfo --help`.

Um zum Beispiel die Daten der eingebauten SCSI-Geräte zu bekommen geben Sie folgenden Befehl ein:

```
hwinfo --scsi
```

Die Ausgaben dieses Hilfsprogrammes stehen Ihnen auch in YaST im Modul Hardware-Information zur Verfügung.

9.4.2 Umgang mit Modulen

Folgende Befehle zum Umgang mit Modulen stehen zur Verfügung:

`insmod` Mit dem Befehl `insmod` wird das angegebene Modul geladen. Das Modul wird in einem Unterverzeichnis von `/lib/modules/<Version>` gesucht. Zugunsten von `modprobe` (s. u.) sollte `insmod` *nicht* mehr verwendet werden.

`rmmod` Entlädt das angegebene Modul. Dies ist natürlich nur dann möglich, wenn die entsprechende Funktionalität des Kernels nicht mehr verwendet wird. So ist es nicht möglich, das Modul `isofs` zu entladen, wenn noch eine CD gemountet ist.

`depmod` Dieser Befehl erzeugt eine Datei mit dem Namen `modules.dep` im Verzeichnis `/lib/modules/<Version>`, in der die Abhängigkeiten der einzelnen Module untereinander verzeichnet sind. Damit stellt man sicher, dass beim Laden eines Modules alle davon abhängigen Module ebenfalls automatisch geladen werden. Die Datei mit den Modul-Abhängigkeiten beim Start des Systems automatisch generiert, sofern sie noch nicht existiert.

`modprobe` Laden bzw. Entladen eines Modules mit Berücksichtigung der Abhängigkeiten von anderen Modulen. Dieser Befehl ist sehr mächtig und kann für eine Reihe weiterer Zwecke eingesetzt werden (etwa Durchprobieren aller Module eines bestimmten Typs, bis eines erfolgreich geladen werden kann). Im Gegensatz zum Laden mittels insmod wertet modprobe die Datei `/etc/modprobe.conf` aus und sollte daher generell zum Laden von Modulen verwendet werden. Für eine ausführliche Erklärung sämtlicher Möglichkeiten lesen Sie bitte die zugehörigen Manual-Pages.

lsmod Zeigt an, welche Module gegenwärtig geladen sind und von wie vielen anderen Modulen sie verwendet werden. Module, die vom Kernel-Daemon geladen wurden, sind durch ein nachfolgendes `autoclean` gekennzeichnet. Die Kennzeichnung mit `autoclean` weist darauf hin, dass diese Module automatisch wieder entfernt werden, wenn sie längere Zeit nicht benutzt wurden und man entsprechende Vorkehrungen getroffen hat; vgl. jedoch Abschnitt 9.4.4.

modinfo Zeigt Informationen zu einem Modul an.

9.4.3 /etc/modprobe.conf

Das Laden von Modulen wird über die Dateien `/etc/modprobe.conf` `/etc/modprobe.conf.local` und das Verzeichnis `/etc/modprobe.d` beeinflusst; vgl. die Manualpage `man modprobe.conf`. In dieser Datei können auch die Parameter für solche Module eingetragen werden, die direkt auf die Hardware zugreifen und daher auf das spezifische System eingestellt werden müssen (zum Beispiel CD-ROM-Treiber oder Netzwerktreiber). Die hier eingetragenen Parameter werden in den Kernel Sourcen beschrieben. Installieren Sie dazu das Paket `kernel-source` und lesen Sie die Dokumentation im Verzeichnis `/usr/src/linux/Documentation/`.

9.4.4 Kmod – der Kernel Module Loader

Der eleganteste Weg bei der Verwendung von Kernel-Modulen ist der Einsatz des „Kernel Module Loader“. Kmod wacht im Hintergrund und sorgt dafür, dass benötigte Module durch modprobe-Aufrufe automatisch geladen werden, sobald auf die entsprechende Funktionalität des Kernels zugegriffen wird.

Um den Kmod verwenden zu können, müssen Sie bei der Kernel-Konfiguration die Option ‘Kernel module loader’ (`CONFIG_KMOD`) aktivieren.

Der Kmod ist nicht dafür ausgelegt, Module wieder automatisch zu entladen; bei der heutigen RAM-Ausstattung der Rechner wäre der Gewinn an Arbeitsspeicher nur marginal. Server-Rechner, die spezielle Aufgaben zu erfüllen haben und nur wenige Treiber benötigen, werden aus Performance-Gründen einen „monolithischen“ Kernel bevorzugen.

9.5 Einstellungen bei der Kernelkonfiguration

Die einzelnen Konfigurationsmöglichkeiten des Kernels können hier nicht im Detail dargestellt werden. Machen Sie bitte Gebrauch von den zahlreich vorhandenen Hilfetexten zur Kernel-Konfiguration. Der neueste Stand der Dokumentation findet sich immer im Verzeichnis `/usr/src/linux/Documentation/` sofern das Paket `kernel-source` installiert ist.

9.6 Übersetzen des Kernels

Wir empfehlen, ein „bzImage“ zu generieren. So lässt es sich in der Regel umgehen, dass der Kernel „zu groß“ wird, wie dies leicht passieren kann, wenn man zu viele Features auswählt und ein „zImage“ herstellt (typisch sind dann die Meldungen "kernel too big" oder "System is too big").

Nachdem Sie den Kernel für Ihre Gegebenheiten konfiguriert haben, starten Sie die Kompilation (in `/usr/src/linux/`:

► **x86**

```
make clean
make bzImage
```

◄

► **POWER**

```
make clean
make vmlinux
```

◄

► **POWER**
Oder für eine RS/6000, wenn ein von Diskette bootbarer Kernel gewünscht wird, zusätzlich `make zImage`. ◄

Diese beiden Befehle können Sie auch in einer Befehlszeile eingeben:

► **x86**

```
make clean bzImage
```

◄

► **POWER**

```
make clean vmlinux
```

◄

► **x86, AMD64, EM64T, IPF, zSeries**
Nach der erfolgreichen Übersetzung finden Sie den komprimierten Kernel in `/usr/src/linux/arch/<arch>/boot/`. Das Kernel-Image – die Datei, die den Kernel enthält – heißt `bzImage`. ◄

► **POWER**
Nach der erfolgreichen Übersetzung finden Sie den Kernel in `/usr/src/linux/`. Das Kernel-Image – die Datei, die den Kernel enthält – heißt `vmlinux`; der Disketten-Kernel für RS/6000 wird jedoch in `/usr/src/linux/arch/<arch>/chrpboot` abgelegt. ◄

Finden Sie diese Datei nicht vor, ist aller Wahrscheinlichkeit nach ein Fehler während der Kernelübersetzung aufgetreten. Unter der Bash können Sie mit:

```
make bzImage 2> &1 | tee kernel.out

make clean vmlinux 2> &1 | tee kernel.out
```

den Kompilationsvorgang erneut starten und in die Datei `kernel.out` „mitschreiben“ lassen.

Wenn Sie Teile des Kernels als ladbare Module konfiguriert haben, müssen Sie anschließend das Übersetzen dieser Module veranlassen. Dies erreichen Sie durch: `make modules`.

9.7 Kernel installieren

Nachdem Sie den Kernel übersetzt haben, müssen Sie dafür sorgen, dass dieser neue Kernel installiert wird, um ihn künftig booten zu können.

► **x86**
Wenn Sie LILO verwenden, so muss dies gleichfalls neu installiert werden. Im einfachsten Fall kopieren Sie dazu den neuen Kernel nach `/boot/vmlinuz` und rufen dann LILO auf; um sich vor unliebsamen Überraschungen zu schützen, empfiehlt es sich jedoch, den alten Kernel zunächst beizubehalten (als `/boot/vmlinuz.old`), um ihn notfalls booten zu können, wenn der neue Kernel nicht wie erwartet funktioniert:

```
cp /boot/vmlinuz /boot/vmlinuz.old
cp arch/i386/boot/bzImage /boot/vmlinuz
lilo
```

Das Makefile-Target `make bzlilo` erledigt diese drei Schritte übrigens in einem Rutsch. ◄

Hinweis

x86:

Wenn Sie GRUB als Bootloader verwenden, muss dieser *nicht* neu installiert werden! Führen Sie also bitte nur die ersten beiden Schritte aus, um den Kernel an die richtige Stelle im System zu kopieren.

Hinweis

► **POWER**

BootX: Die bereits genannte Datei `vmlinux` ist nach 'Linux Kernels' in den Systemordner zu kopieren. Beim nächsten Start von BootX ist der neue Kernel auszuwählen und auf 'Save to prefs' zu klicken.

RS/6000 (quik): `vmlinux` ist nach `/boot` zu kopieren und `/etc/quik.conf` ist anzupassen.

RS/6000 (Diskette): Das `zImage` ist aus dem Verzeichnis `/usr/src/linux/arch/<arch>/chrpboot` auf auf eine DOS-Diskette zu kopieren.

◄

Die übersetzten Module müssen nun noch installiert werden; durch Eingabe von `make modules_install` können Sie diese in die korrekten Zielverzeichnisse unter `/lib/modules/<Version>/` kopieren lassen. Dabei werden die alten Module bei gleicher Kernelversion überschrieben; Sie können jedoch die ursprünglichen Module zusammen mit dem Kernel von den CDs wieder installieren.

Hinweis

Es ist darauf zu achten, dass Module, deren Funktionalität man jetzt eventuell direkt in den Kernel einkompiliert hat, unter `/lib/modules/<Version>/` entfernt werden. Sonst kann es zu unvorhersehbaren Effekten kommen! Dies ist ein Grund, weshalb dem Ungeübten vom Selbstkompilieren des Kernels *dringend* abgeraten wird.

Hinweis

► **x86**
Damit der alte Kernel (jetzt `/boot/vmlinuz.old`) von GRUB oder LILO gebootet werden kann, tragen Sie in der Datei `/boot/grub/menu.lst` bzw. in `/etc/lilo.conf` zusätzlich ein Label `Linux.old` als Boot-Image ein. Dieses Vorgehen wird ausführlich im Kapitel 8 auf Seite 223 beschrieben. Falls Sie LILO als Bootloader verwenden, müssen Sie nach den Anpassungen in `/etc/lilo.conf` erneut `lilo` aufrufen. Bei GRUB ist keine Neuinstallation notwendig.

Weiterhin ist Folgendes zu beachten: Die Datei `/boot/System.map` enthält die Kernelsymbole, die die Kernelmodule benötigen, um Kernelfunktionen korrekt aufrufen zu können. Diese Datei ist abhängig vom aktuellen Kernel. Daher sollten Sie nach der Übersetzung und Installation des Kernels die aktuelle Datei `/usr/src/linux/System.map` in das Verzeichnis `/boot/` kopieren. Bei jeder Kernelübersetzung wird diese Datei neu erzeugt. Falls Sie Ihren Kernel mittels `make bzlilo` bzw. `make zlilo` erstellen, wird diese Aufgabe automatisch für Sie erledigt.

Sollten Sie beim Booten eine Fehlermeldung wie "System.map does not match actual kernel" erhalten, dann wurde wahrscheinlich nach der Kernelübersetzung die Datei `System.map` nicht nach `/boot/` kopiert. ◄

9.8 Festplatte nach der Übersetzung aufräumen

Sie können die während der Kernel-Übersetzung erzeugten Objekt-Dateien löschen, falls Sie Probleme mit dem Plattenplatz haben:

```
cd /usr/src/linux
make clean
```

Falls Sie jedoch über ausreichend Plattenplatz verfügen und vorhaben, den Kernel des Öfteren neu zu konfigurieren, so überspringen Sie diesen letzten Schritt. Ein erneutes Übersetzen des Kernels ist dann erheblich schneller, da nur die Teile des Systems neu übersetzt werden, die von den entsprechenden Änderungen betroffen sind.

Systemmerkmale

In diesem Kapitel finden Sie Hinweise zu *Filesystem Hierarchy Standard* (FHS) und *Linux Standard Base* (LSB). Einzelne Softwarepakete und besondere Eigenheiten wie das Booten mit der `initrd`, das Programm linuxrc und das Rettungssystem werden detailliert beschrieben.

10.1 Linux-Standards 268
10.2 Hinweise zu speziellen Softwarepaketen 269
10.3 Booten mit der initial ramdisk 275
10.4 Das SUSE Rettungssystem 280
10.5 Virtuelle Konsolen 284
10.6 Tastaturbelegung 285
10.7 Lokale Anpassungen — I18N/L10N 286

10.1 Linux-Standards

10.1.1 Linux Standard Base (LSB)

SUSE unterstützt aktiv die Bemühungen des *Linux Standard Base*-Projekts; aktuelle Informationen dazu unter `http://www.linuxbase.org`.

Die LSB-Spezifikation liegt in der Version 1.3.x vor. Nunmehr ist der Filesystem Hierarchy Standard (FHS) Teil der Spezifikation und es sind u. a. das Paketformat und die Initialisierung des Systems festgelegt; vgl. Kapitel 11 auf Seite 289.

10.1.2 Filesystem Hierarchy Standard (FHS)

SUSE LINUX ist gemäß LSB-Spezifikation konform zum *Filesystem Hierarchy Standard* (FHS, `fhs`-Paket); vgl. `http://www.pathname.com/fhs/`. Aus diesem Grunde war es bisweilen erforderlich, Dateien oder Verzeichnisse an die richtigen Stelle zu verschieben, wie diese im FHS festgelegt ist.

Ein Ziel des FHS ist es beispielsweise, eine Struktur zu definieren, mit deren Hilfe es möglich ist, `/usr` read-only einzuhängen (mounten).

10.1.3 teTeX — TeX unter SuSE Linux

TeX ist ein komplexes Satzsystem, das auf zahlreichen Plattformen läuft. Es ist über Makro-Pakete wie LaTeX erweiterbar. Es besteht aus sehr vielen einzelnen Dateien, die gemäß der *TeX Directory Structure* (TDS) zusammenzustellen sind (vgl. `ftp://ftp.dante.de/tex-archive/tds/`; teTeX ist eine Zusammenstellung aktueller TeX-Software.

Unter SUSE LINUX kommt teTeX in einer Konfiguration zum Einsatz, die sowohl die Anforderungen des TDS als auch des FHS erfüllt.

10.1.4 Zu FTP

Um die Einrichtung eines FTP-Servers zu erleichtern, hält das Paket `ftpdir` eine Beispielumgebung bereit. Diese Umgebung wird unter `/srv/ftp` installiert.

10.1.5 Zu HTTP

Apache ist der Standard-Webserver bei SUSE LINUX. Gleichzeitig mit der Installation des Apache werden Beispiel-Dokumente unter `/srv/www/` zur Verfügung gestellt. Wenn Sie einen eigenen Webserver aufbauen wollen, tragen Sie bitte eine eigene `DocumentRoot` in `/etc/httpd/httpd.conf` ein und legen Sie dort Ihre Dateien (Dokumente, Bilder etc.) ab.

10.2 Hinweise zu speziellen Softwarepaketen

10.2.1 Paket bash und /etc/profile

In dieser Reihenfolge wertet die bash die Initialisierungsdateien aus, wenn sie als Loginshell aufgerufen wird:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Eigene Einträge können Benutzer in `~/.profile` bzw. `~/.bashrc` vornehmen. Um ordnungsgemäßes Abarbeiten dieser Dateien zu gewährleisten, ist es erforderlich, dass die aktuellen Grundeinstellungen von `/etc/skel/.profile` bzw. `/etc/skel/.bashrc` in das Benutzerverzeichnis übernommen werden. Nach einem Update empfiehlt sich deshalb, die Einstellungen aus `/etc/skel` zu übernehmen. Um keine eigenen Anpassungen zu verlieren, führen Sie bitte die folgenden Shellbefehle aus:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Danach sind die eigenen Anpassungen aus den Dateien `*.old` zurückzuschreiben.

10.2.2 Paket cron

Die cron-Tabellen liegen unter /var/spool/cron/tabs. Als systemweite Tabelle wird die Datei /etc/crontab eingerichtet. In der Datei /etc/crontab muss zusätzlich nach der Zeitangabe eingetragen werden, unter welchem Benutzer der jeweilige Auftrag ausgeführt werden soll (vgl. Datei 10.1, dort ist root angegeben); dem gleichen Format folgen paketspezifische Tabellen, die in /etc/cron.d/ liegen – vgl. die Manualpage man cron.

Beispiel 10.1: *Beispiel eines Eintrags in /etc/crontab*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

/etc/crontab kann *nicht* mit crontab -e bearbeitet werden, sondern muss direkt in einen Editor geladen, bearbeitet und gespeichert werden.

Einige Pakete installieren in den Verzeichnissen /etc/cron.hourly/, /etc/cron.daily/, /etc/cron.weekly/ und /etc/cron.monthly/ Shellskripten, deren Abarbeitung von /usr/lib/cron/run-crons gesteuert wird. /usr/lib/cron/run-crons wird alle 15 Minuten von der Haupt-Tabelle (/etc/crontab) aufgerufen. So wird sichergestellt, dass eventuell versäumte Läufe rechtzeitig nachgeholt werden.

Die täglichen Wartungsarbeiten am System sind aus Gründen der Übersichtlichkeit auf mehrere Skripten verteilt worden (Paket aaa_base). In /etc/cron.daily/ gibt es also neben aaa_base zum Beispiel die Komponenten backup-rpmdb, clean-tmp oder clean-vi.

10.2.3 Protokoll-Dateien — das Paket logrotate

Zahlreiche System-Dienste (engl. *Daemons*) und auch der Kernel selbst protokollieren regelmäßig Systemzustände oder besondere Vorkommnisse in Protokoll-Dateien (engl. *logfiles*). So kann der Administrator zuverlässig feststellen, in welchem Zustand sich das System zu einem bestimmten Zeitpunkt befand, Fehler oder Fehlfunktionen erkennen und gezielt beheben. Diese Protokoll-Dateien werden in der Regel gemäß FHS unter /var/log abgelegt und werden von Tag zu Tag größer. Mit Hilfe von logrotate ist es möglich, das Wachsen der Protokoll-Dateien zu steuern.

Konfiguration

In der Konfigurationsdatei `/etc/logrotate.conf` wird das generelle Verhalten festgelegt. Mit der `include`-Angabe wird insbesondere konfiguriert, welche weiteren Dateien ausgewertet werden sollen. Bei SUSE LINUX ist vorgesehen, dass die einzelnen Pakete in `/etc/logrotate.d` Dateien installieren (beispielsweise `syslog` oder `yast`).

Beispiel 10.2: *Beispiel für /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly weekly
# keep 4 weeks worth of backlogs rotate 4
# create new (empty) log files after rotating old ones create
# uncomment this if you want your log files compressed
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}
# system-specific logs may be also be configured here.
```

logrotate selbst wird über cron gesteuert und einmal täglich von `/etc/cron.daily/logrotate` angestoßen.

Hinweis

Die Option `create` liest etwaige Einstellungen des Administrator in den Dateien `/etc/permissions*` ein. Stellen Sie bitte sicher, dass es bei eigenen Anpassungen zu keinen Konflikten kommt.

Hinweis

10.2.4 Manual-Pages

Für einige GNU-Programme (zum Beispiel tar) werden die Manual-Pages nicht mehr weiter gepflegt. An ihre Stelle treten als Schnellübersicht die `--help`-Ausgabe sowie als ausführliche Handbücher die Info-Dateien. info ist GNUs Hypertext-System. Mit `info info` erhält man erste Hilfe zur Benutzung; info kann entweder über Emacs `emacs -f info` aufgerufen werden, oder direkt mit dem Befehl `info`. Angenehm zu bedienen sind tkinfo, xinfo oder der Zugriff über das Hilfesystem.

10.2.5 Der Befehl ulimit

Mit dem Befehl `ulimit` (engl. *user limits*) ist es möglich, Limits für die Nutzung von Systemressourcen zu setzen, bzw. sich diese anzeigen zu lassen. Insbesondere ist ulimit dazu geeignet, den zur Verfügung stehenden Speicher für Anwendungen zu begrenzen. Dadurch wird verhindert, dass eine Anwendung übermäßig viel (allen) Speicherplatz für sich beschlagnahmt und das System zum Stillstand kommt.

Der Aufruf von ulimit kann mit verschiedenen Optionen erfolgen. Um den Speicherverbrauch zu begrenzen, sind zum Beispiel die Optionen in Tabelle 10.1 tauglich.

Tabelle 10.1: *ulimit: Ressourcen für den Anwender einstellen*

`-m`	max. Größe des physikalischen Speichers
`-v`	max. Größe des virtuellen Speichers
`-s`	max. Größe des Stacks
`-c`	max. Größe der Core-Dateien
`-a`	Anzeige der gesetzten Limits

Systemweit können die Einstellungen in `/etc/profile` vorgenommen werden. Dort muss beispielsweise das Erzeugen von Core-Dateien freigeschaltet werden, die Programmierer zum „Debuggen“ benötigen. Als Anwender kann man die vom Systemadministrator in `/etc/profile` vorgegebenen Werte nicht erhöhen, aber man kann spezielle Einstellung in die eigene `~/.bashrc` eintragen.

Beispiel 10.3: *ulimit-Einstellungen in /.bashrc*

```
# Begrenzung des realen Speichers
ulimit -m 98304

# Begrenzung des virtuellen Speichers
ulimit -v 98304
```

Die Speicherangaben müssen in KB gemacht werden. Für detailliertere Informationen werfen Sie bitte einen Blick in die Manualpage `man bash`.

Hinweis

Nicht alle Shells unterstützen `ulimit`-Angaben. Wenn Sie auf übergreifende Einstellungen für derartige Beschränkungen angewiesen sind, dann bietet PAM (zum Beispiel `pam_limits`) weitgehende Einstellmöglichkeiten.

Hinweis

10.2.6 Der Befehl free

Der Befehl `free` ist etwas irreführend, wenn es darum geht herauszufinden, wie der Arbeitsspeicher gerade verwendet wird … Informationen findet man in `/proc/meminfo`. Heutzutage sollte sich eigentlich kein Anwender darum Gedanken machen, dem ein modernes Betriebssystem wie Linux zur Verfügung steht. Das Konzept vom „freien Arbeitsspeicher“ datiert von der Zeit her, als es noch keine vereinheitlichte Speicherverwaltung (engl. *unified memory management*) gab – unter Linux gilt das Motto: „freier Speicher ist schlechter Speicher“ (engl. *free memory is bad memory*). Infolgedessen ist Linux immer bestrebt, verschiedene Caches auszubalancieren, nie aber wirklich freien (= ungenutzten) Speicher zuzulassen.

Der Kernel weiß im Grunde nichts direkt von Programmen oder Benutzerdaten. Er verwaltet Programme und Benutzerdaten im so genannten „Page Cache“. Wenn der Speicher knapp wird, werden Teile davon entweder in den Swapbereich oder in die Dateien geschrieben, aus denen sie ursprünglich mit Hilfe des Systemaufrufs `mmap` gelesen wurden; vgl. die Manualpage von `mmap`.

Des Weiteren hält der Kernel auch noch andere Zwischenspeicher, wie den „slab cache“, der zum Beispiel die für den Netzwerkzugriff benutzten Puffer enthält. Dadurch werden eventuelle Differenzen zwischen den Zählern in `/proc/meminfo` erklärt. Die meisten, aber nicht alle, sind über `/proc/slabinfo` abfragbar.

10.2.7 Die Datei /etc/resolv.conf

Die Namensauflösung wird über die Datei `/etc/resolv.conf` geregelt; vgl.Abschnitt 21.7 auf Seite 502 . Diese Datei wird stets nur von dem Skript `/sbin/modify_resolvconf` aktualisiert. Es ist keinem Programm erlaubt, `/etc/resolv.conf` direkt zu manipulieren. Nur wenn diese Regel beachtet wird, kann sichergestellt werden, dass die Netzwerkkonfiguration und die zugehörigen Daten konsistent gehalten werden.

10.2.8 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. Weiterführende Informationen finden Sie unter `http://www.gnu.org/software/emacs/`.

In den folgenden Absätzen werden die Konfigurationsdateien genannt, die GNU Emacs beim Start abarbeitet. Beim Start liest Emacs mehrere Dateien ein, um gemäß den Vorgaben des Benutzers, des Systemadministrators und oder des Distributors für die jeweilige Bedürfnissen angepasst oder vorkonfiguriert zu werden.

Für jeden Benutzer wird im Home-Verzeichnis die Initialisierungsdatei `~/.emacs` von `/etc/skel/` installiert; `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs` ein. Wenn ein Benutzer eigene Anpassungen vornehmen möchte, empfiehlt es sich, diese Datei `.gnu-emacs` in das eigene Home-Verzeichnis zu kopieren und dort die gewünschten Einstellungen vorzunehmen:

```
cp /etc/skel/.gnu-emacs ~/.gnu-emacs
```

In `.gnu-emacs` wird die Datei `~/.gnu-emacs-custom` als `custom-file` festgelegt; wenn der Benutzer mit den `customize`-Möglichkeiten eigene Einstellungen vornimmt, werden diese in `~/.gnu-emacs-custom` gespeichert.

Mit dem Paket `emacs` wird bei SUSE LINUX die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird *vor* der Initialisierungsdatei `~/.emacs` geladen. `site-start.el` sorgt beispielsweise dafür, dass besondere Konfigurationsdateien automatisch geladen werden, die mit Emacs-Zusatzpaketen der Distribution installiert werden (zum Beispiel Paket `psgml`). Derartige Konfigurationsdateien befinden sich gleichfalls in `/usr/share/emacs/site-lisp` und beginnen stets mit `suse-start-`.

Der lokale Systemadministrator kann in `default.el` systemweite Einstellungen vornehmen. Mehr Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs, im Knoten `Init File`: `info:/emacs/InitFile`. Dort ist auch beschrieben, wie man — falls notwendig — das Laden dieser Dateien verhindern kann.

Die Bestandteile des Emacs' sind auf mehrere Pakete verteilt:

- Basispaket `emacs`

- Dazu ist in der Regel das Paket `emacs-x11` zu installieren, in dem das Programm *mit* X11-Unterstützung enthalten ist.
- Im Paket `emacs-nox` ist das Programm *ohne* X11-Unterstützung enthalten.
- Das Paket `emacs-info` stellt Online-Dokumentation im Info-Format bereit.
- Das Paket `emacs-el` enthält die nicht kompilierten Bibliotheksdateien in Emacs Lisp — zur Laufzeit nicht erforderlich!
- Zahlreiche Zusatzpakete, die nach Bedarf installiert werden können: Paket `emacs-auctex` (für LaTeX); `psgml` (für SGML/XML); `gnuserv` (für Client-/Serverbetrieb) usw.

10.3 Booten mit der initial ramdisk

10.3.1 Problemstellung

Sobald der Linux-Kernel geladen und das Root-Dateisystem (`/`) gemountet ist, können Programme ausgeführt und weitere Kernel-Module eingebunden werden, um zusätzliche Funktionalitäten bereitzustellen. Um aber das Root-Dateisystem überhaupt mounten zu können, müssen verschiedene Bedingungen erfüllt sein: Der Kernel benötigt die entsprechenden Treiber, um das Gerät ansprechen zu können, auf dem das Root-Dateisystem liegt (insbesondere SCSI-Treiber). Weiter muss der Kernel den Code enthalten, der benötigt wird, um das Dateisystem lesen zu können (`ext2`, `reiserfs`, `romfs` usw.). Weiterhin ist es denkbar, dass bereits das Root-Dateisystem verschlüsselt ist. Zum Mounten ist in diesem Fall die Eingabe des Schlüssels/Passworts erforderlich.

Betrachtet man nur einmal das Problem der SCSI-Treiber, so sind verschiedene Lösungsansätze denkbar: Der Kernel kann alle denkbaren Treiber enthalten. Dies ist problematisch, da sich die verschiedenen Treiber beißen können. Außerdem wird der Kernel dadurch sehr groß. Eine andere Möglichkeit besteht darin, verschiedene Kernel zur Verfügung zu stellen, die jeweils nur einen oder sehr wenige SCSI-Treiber enthalten. Auch dieser Weg ist problematisch, da er eine sehr große Zahl unterschiedlicher Kernel notwendig macht. Ein Problem, das durch verschieden optimierte Kernel (Athlon-Optimierung, SMP) noch weiter verschärft wird.

Der Ansatz, den SCSI-Treiber als Modul zu laden, führt zur generellen Problematik, der durch das Konzept der *initial ramdisk* begegnet wird: Das Bereitstellen einer Möglichkeit, Userspace-Programme bereits vor dem Mounten des Root-Dateisystems ausführen zu können.

10.3.2 Konzept der initial ramdisk

Die *initial ramdisk* (auch initdisk oder initrd genannt) löst genau diese oben beschriebenen Probleme. Der Linux-Kernel bietet die Möglichkeit, ein (kleines) Dateisystem in eine Ramdisk zu laden, und darin Programme ausführen zu lassen, bevor das eigentliche Root-Dateisystem gemountet wird. Das Laden der `initrd` wird dabei vom Bootloader (GRUB, LILO usw.) übernommen; all diese Bootloader benötigen lediglich BIOS-Routinen, um Daten vom Bootmedium zu laden. Wenn der Bootloader den Kernel laden kann, kann er auch die initial ramdisk laden. Spezielle Treiber sind somit nicht erforderlich.

10.3.3 Ablauf des Bootvorgangs mit initrd

Der Bootloader lädt den Kernel und die `initrd` in den Speicher und startet den Kernel, wobei der Bootloader dem Kernel mitteilt, dass eine `initrd` vorhanden ist und wo im Speicher diese liegt. Ist die `initrd` komprimiert (was typischerweise der Fall ist), so dekomprimiert der Kernel die `initrd` und mountet sie als temporäres Root-Dateisystem. Hierauf wird in der `initrd` ein Programm mit dem Namen linuxrc gestartet. Dieses Programm kann nun all die Sachen tun, die erforderlich sind, um das richtige Root-Dateisystem mounten zu können. Sobald linuxrc terminiert, wird die (temporäre) `initrd` wieder abgehängt (engl. *unmounted*) und der Bootvorgang wie gewohnt mit dem Mounten des richtigen Root-Dateisystems fortgeführt. Das Mounten der `initrd` und das Ausführen von linuxrc kann somit als ein kurzes Intermezzo während eines normalen Bootvorgangs betrachtet werden. Der Kernel versucht nach dem Booten der tatsächlichen Root-Partition, die `initrd` auf das Verzeichnis `/initrd` umzumounten. Wenn das fehlschlägt, weil zum Beispiel der Mountpunkt `/initrd` nicht vorhanden ist, wird der Kernel versuchen, die `initrd` abzuhängen. Sollte auch dies fehlschlagen, ist das System zwar voll funktionsfähig, jedoch kann der durch die `initrd` belegte Speicher nie freigegeben werden; er steht somit nicht mehr zur Verfügung.

Das Programm linuxrc

Für das Programm linuxrc in der `initrd` gibt es lediglich die folgenden Anforderungen: Das Programm muss den speziellen Namen `linuxrc` tragen und im Root-Verzeichnis der `initrd` liegen. Abgesehen davon muss es lediglich vom Kernel ausgeführt werden können. Das bedeutet, dass linuxrc durchaus dynamisch gelinkt sein darf. In diesem Fall müssen natürlich die shared libraries wie gewohnt vollständig unter `/lib` in der `initrd` verfügbar sein. Weiter darf linuxrc auch ein Shellskript sein. In diesem Fall muss natürlich eine Shell in `/bin` existieren. Kurz gesagt, muss die `initrd` ein minimales Linux-System enthalten, das die Ausführung des Programmes linuxrc erlaubt. Bei der Installation von SUSE LINUX wird ein statisch gelinktes linuxrc verwendet, um die `initrd` so klein wie möglich halten zu können. linuxrc wird mit `root`-Rechten ausgeführt.

Das echte Root-Dateisystem

Sobald linuxrc terminiert, wird die `initrd` abgehängt und verworfen, der Bootvorgang geht normal weiter und der Kernel mountet das wirkliche Root-Dateisystem. Was als Root-Dateisystem gemountet werden soll, kann durch linuxrc beeinflusst werden. Dazu muss linuxrc lediglich das `/proc`-Dateisystem mounten und den Wert des echten Root-Dateisystems in numerischer Form nach `/proc/sys/kernel/real-root-dev` schreiben.

10.3.4 Bootloader

Die meisten Bootloader (vor allem GRUB, LILO und syslinux) können mit `initrd` umgehen. Die einzelnen Bootloader werden wie folgt angewiesen, eine `initrd` zu verwenden:

GRUB Eintrag der folgenden Zeile in `/boot/grub/menu.lst`:

```
initrd (hd0,0)/initrd
```

Da die Ladeadresse der initrd in das bereits geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den `kernel`-Befehl folgen.

LILO Eintrag der folgenden Zeile in `/etc/lilo.conf`:

```
initrd=/boot/initrd
```

Die Datei `/boot/initrd` ist die *initial ramdisk*. Sie kann komprimiert sein.

syslinux Eintrag der folgenden Zeile in `syslinux.cfg`:

```
append initrd=initrd
```

Weitere Parameter können in der Zeile folgen.

10.3.5 Anwendung von initrd bei SUSE

Installation des Systems

Die `initrd` wird bereits seit geraumer Zeit für die Installation verwendet: Bei manueller Installation kann der Anwender in linuxrc Kernel-Module laden und die für eine Installation notwendigen Eingaben vornehmen. linuxrc startet dann YaST, das die Installation durchführt. Hat YaST seine Arbeit getan, teilt es linuxrc mit, wo das Root-Dateisystem des frisch installierten Systems liegt. linuxrc schreibt diesen Wert nach `/proc` und führt dann einen Reboot durch. Danach startet YaST erneut und installiert die restlichen Pakete bereits in jenes System, das gerade installiert wird.

Booten des installierten Systems

In der Vergangenheit hat YaST mehr als 40 Kernel für die Installation im System angeboten, wobei sich die Kernel im Wesentlichen dadurch unterschieden, dass jeder Kernel einen bestimmten SCSI-Treiber enthielt. Dies war nötig, um nach dem Booten das Root-Dateisystem mounten zu können. Weitere Treiber konnten dann als Modul nachgeladen werden.

Da inzwischen aber auch optimierte Kernel zur Verfügung gestellt werden, ist dieses Konzept nicht mehr tragbar – es wären inzwischen weit über 100 Kernel-Images nötig.

Daher wird nun auch für das normale Starten des Systems eine `initrd` verwendet. Die Funktionsweise ist analog zu einer Installation. Das hier eingesetzte linuxrc ist jedoch einfach nur ein Shellskript, das lediglich die Aufgabe hat, einige vorgegebene Module zu laden. Typischerweise handelt es sich nur um ein einziges Modul, nämlich denjenigen SCSI-Treiber, der benötigt wird, um auf das Root-Dateisystem zugreifen zu können.

Erstellen einer initrd

Das Erstellen einer `initrd` erfolgt mittels des Skripts `mkinitrd` (früher `mk_initrd`). Die zu ladenden Module werden bei SUSE LINUX durch die Bezeichner `INITRD_MODULES` in `/etc/sysconfig/kernel` festgelegt. Nach einer Installation wird diese Variable automatisch durch die richtigen

Werte vorbelegt (das Installations-linuxrc weiß ja, welche Module geladen wurden). Die Module werden in genau der Reihenfolge geladen, in der sie in `INITRD_MODULES` auftauchen. Das ist besonders wichtig, wenn mehrere SCSI-Treiber verwendet werden, da sich ansonsten die Benennung der Platten ändern würde. Streng genommen würde es reichen, nur denjenigen SCSI-Treiber laden zu lassen, der für den Zugriff auf das Root-Dateisystem benötigt wird. Da das automatische Nachladen zusätzlicher SCSI-Treiber jedoch problematisch ist, laden wir alle bei der Installation verwendeten SCSI-Treiber mittels der `initrd`.

Hinweis

Da das Laden der `initrd` durch den Bootloader genauso abläuft wie das Laden des Kernels selbst (LILO vermerkt in seiner `map`-Datei die Lage der Dateien), muss bei der Verwendung von LILO nach jeder Änderung der `initrd` der Bootloader neu installiert werden – bei der Verwendung von GRUB ist dies nicht notwendig!

Hinweis

10.3.6 Mögliche Schwierigkeit – Selbstkompilierte Kernel

Übersetzt man sich selbst einen Kernel, so kann es zu folgendem Problem kommen: Versehentlich wird der SCSI-Treiber fest in den Kernel gelinkt, die bestehende `initrd` bleibt aber unverändert. Beim Booten geschieht Folgendes: Der Kernel enthält bereits den SCSI-Treiber, die Hardware wird erkannt. Die `initrd` versucht nun jedoch, den Treiber nochmals als Modul zu laden. Dies führt bei einigen SCSI-Treibern (insbesondere beim `aic7xxx`) zum Stillstand des Systems. Streng genommen handelt es sich um einen Kernelfehler (ein bereits vorhandener Treiber darf nicht ein zweites Mal als Modul geladen werden können) – das Problem ist bereits im Zusammenhang mit seriellen Treibern bekannt.

Es gibt mehrere Lösungen: Entweder den Treiber als Modul konfigurieren (dann wird er korrekt in der `initrd` geladen) oder aber den Eintrag für die `initrd` aus `/etc/grub/menu.lst` bzw. `/etc/lilo.conf` entfernen. Äquivalent zur letzteren Lösung ist es, den Treiber aus `INITRD_MODULES` zu entfernen und `mkinitrd` aufzurufen, das dann feststellt, dass keine `initrd` benötigt wird.

10.3.7 Ausblick

Für die Zukunft ist denkbar, dass eine `initrd` für weitaus mehr (und anspruchsvollere) Dinge verwendet wird als nur für das Laden der Module, die für den Zugriff auf `/` benötigt werden.

- Root-Dateisystem auf Software RAID (linuxrc setzt die `md`-Devices auf)
- Root-Dateisystem auf LVM
- Root-Dateisystem ist verschlüsselt (linuxrc fragt nach Passwort)
- Root-Dateisystem auf einer SCSI-Platte am PCMCIA-Adapter

Weitere Informationen

- `/usr/src/linux/Documentation/initrd.txt`
  (Nur verfügbar, wenn die Kernel-Quellen installiert wurden)
- Die man-page zu initrd.

10.4 Das SUSE Rettungssystem

SUSE LINUX enthält ein Rettungssystem, mit dessen Hilfe Sie in Notfällen von außen auf Ihre Linux-Partitionen zugreifen können: Sie können das *Rescue–System* von CD, Netzwerk oder vom SUSE-FTP-Server laden. Weiterhin gibt es eine bootbare SUSE LINUX–CD (die *LiveEval-CD*), die als Rettungssystem eingesetzt werden kann. Zum Rettungssystem gehören verschiedene Hilfsprogramme, mit denen Sie Probleme mit unzugänglich gewordenen Festplatten, fehlerhaften Konfigurationsdateien usw. beheben können. Teil des Rettungssystems ist auch Parted (`parted`) zum Verändern der Partitionsgrößen. Es kann bei Bedarf aus dem Rettungssystem heraus manuell aufgerufen werden, falls Sie nicht auf den in YaST integrierten Resizer zurückgreifen wollen. Informationen zu Parted finden Sie unter:

`http://www.gnu.org/software/parted/`

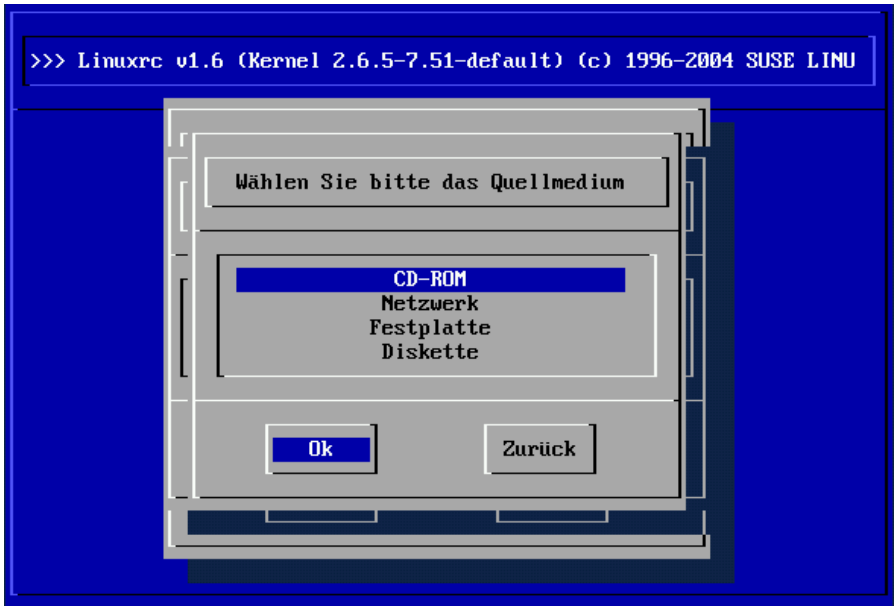

Abbildung 10.1: *Quellmedium für das Rettungssystem*

10.4.1 Das Rettungssystem starten

Das Rettungssystem wird von CD (oder DVD) gestartet. Voraussetzung ist, dass das CD-ROM/DVD-Laufwerk bootfähig ist. Gegebenenfalls müssen Sie im BIOS-Setup die Boot-Reihenfolge ändern.

Nachfolgend die Schritte zum Starten des Rettungssystems:

1. Legen Sie die die erste CD oder DVD von SUSE LINUX in das entsprechende Laufwerk ein und schalten Sie Ihr System ein.
2. Sie können entweder das System durchbooten lassen oder Sie wählen 'Manual Installation' aus, und können dann – falls notwendig – bei 'boot option' spezielle Boot-Parameter angeben.
3. Nehmen Sie im linuxrc die erforderlichen Einstellungen für die Sprache und die Tastatur vor.
4. Anschließend können die für ihr System benötigten Kernel-Module geladen werden. Laden Sie hier bitte *alle* Module, von denen Sie glau-

ben, dass sie später im Rettungssystem gebraucht werden. Das Rettungssystem selbst enthält aus Platzgründen fast keine.

5. Wählen Sie im Hauptmenü den Punkt 'Installation/System starten'.

6. Wählen Sie im Menü 'Installation/System starten' den Punkt 'Rettungssystem starten' (s. Abb. 3.7 auf Seite 133) und geben Sie dann das gewünschte Quellmedium an (s. Abb. 10.1 auf der vorherigen Seite).

   'CD-ROM' Das Rettungssystem auf der CD-ROM wird verwendet.

   'Netzwerk' Das Rettungssystem wird über eine Netzverbindung gestartet. Hierfür muss vorher das richtige Kernel-Modul für die Netzwerkkarte geladen worden sein (vgl. die allgemeinen Hinweise in Abschnitt 3.5.2 auf Seite 141). In einem Untermenü stehen mehrere Protokolle zur Verfügung (s. Abb. 10.2): NFS, FTP, SMB etc.

   'Festplatte' Sollten Sie vorher schon ein Rettungssystem auf eine aktuell erreichbare Festplatte kopiert haben, können Sie hier angeben wo es liegt. Dieses Rettungssystem wird dann verwendet.

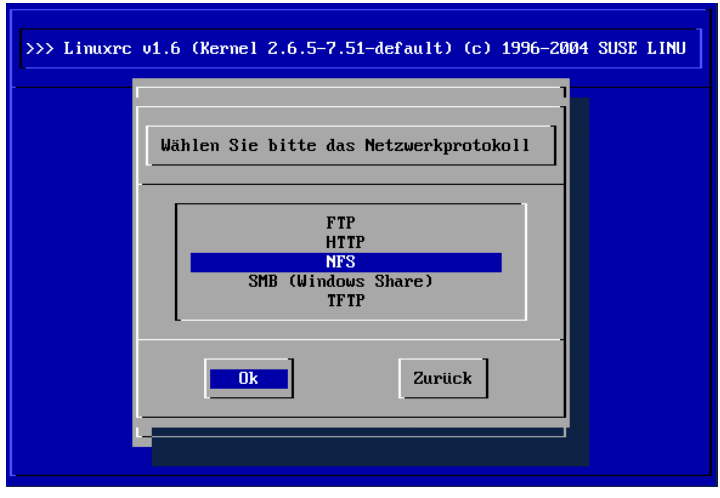

Abbildung 10.2: *Netzwerkprotokolle*

Welches Medium Sie auch gewählt haben, das Rettungssystem wird dekomprimiert, als neues Root-Dateisystem in eine RAM-Disk geladen, gemountet und gestartet. Es ist damit betriebsbereit.

10.4.2 Das Rettungssystem benutzen

Das Rettungssystem stellt Ihnen unter (Alt) + (F1) bis (Alt) + (F3) mindestens drei virtuelle Konsolen zur Verfügung, an denen Sie sich als Benutzer `root` ohne Passwort einloggen können. Mit (Alt) + (F10) kommen Sie zur Systemkonsole mit den Meldungen von Kernel und syslog.

In dem Verzeichnis `/bin` finden Sie die Shell und Utilities (zum Beispiel mount). Wichtige Datei- und Netz-Utilities, zum Beispiel zum Überprüfen und Reparieren von Dateisystemen (reiserfsck, e2fsck etc.), liegen im Verzeichnis `/sbin`. Des Weiteren finden Sie in diesem Verzeichnis auch die wichtigsten Binaries für die Systemverwaltung wie fdisk, mkfs, mkswap, init, shutdown, sowie für den Netzwerkbetrieb ifconfig, route und netstat. Als Editor ist der vi unter `/usr/bin` verfügbar; hier sind auch weitere Tools (grep, find, less etc.) wie auch das Programm telnet zu finden.

Zugriff auf das normale System

Zum Mounten Ihres SUSE LINUX-Systems auf der Platte ist der Mountpoint `/mnt` gedacht. Sie können für eigene Zwecke weitere Verzeichnisse erzeugen und als Mount-Punkte verwenden.

Nehmen wir als Beispiel einmal an, Ihr normales System setzt sich laut `/etc/fstab` wie in der Beispieldatei 10.4 beschrieben zusammen.

Beispiel 10.4: *Beispiel /etc/fstab*

```
/dev/sdb5       swap        swap        defaults   0   0
/dev/sdb3       /           ext2        defaults   1   1
/dev/sdb6       /usr        ext2        defaults   1   2
```

Achtung

Beachten Sie im folgendem Abschnitt die Reihenfolge, in welcher die einzelnen Geräte zu mounten sind.

Achtung

Um Zugriff auf Ihr gesamtes System zu haben, mounten Sie es Schritt für Schritt unter `/mnt` mit den folgenden Befehlen:

```
mount /dev/sdb3 /mnt
mount /dev/sdb6 /mnt/usr
```

Nun haben Sie Zugriff auf Ihr ganzes System und können zum Beispiel Fehler in Konfigurationsdateien wie `/etc/fstab`, `/etc/passwd`, `/etc/inittab` beheben. Die Konfigurationsdateien befinden sich statt im Verzeichnis `/etc` jetzt im Verzeichnis `/mnt/etc`. Um selbst komplett verloren gegangene Partitionen mit dem Programm fdisk einfach wieder durch Neu-Anlegen zurückzugewinnen, sollten Sie sich *vorher* einen Ausdruck (Hardcopy) von dem Verzeichnis `/etc/fstab` und dem Output des Befehls `fdisk -l` machen.

Dateisysteme reparieren

Beschädigte Dateisysteme sind ein besonders ernster Anlass für den Griff zum Rettungssystem. Dateisysteme lassen sich grundsätzlich nicht im laufenden Betrieb reparieren. Bei schwereren Schäden lässt sich unter Umständen nicht einmal mehr das Root-Dateisystem mounten und der Systemstart endet in einer `kernel panic`. Dann bleibt nur noch der Weg, die Reparatur von außen unter einem Rettungssystem zu versuchen.

Im SUSE LINUX-Rettungssystem sind die Utilities reiserfsck, e2fsck und dumpe2fs (zur Diagnose) enthalten. Damit beheben Sie die meisten Probleme. Und da auch im Notfall oft die Manual-Page von reiserfsck oder e2fsck nicht mehr zugänglich ist, sind sie im Anhang C auf Seite 807 bzw. B auf Seite 801 ausgedruckt.

Beispiel: Wenn sich ein `ext2`-Dateisystem wegen eines *ungültigen Superblocks* nicht mehr mounten lässt, wird das Programm e2fsck vermutlich zunächst ebenfalls scheitern. Die Lösung ist, die im Dateisystem alle 8192 Blöcke (8193, 16385...) angelegt und gepflegten Superblock-Backups zu verwenden. Dies leistet zum Beispiel der Befehl:

```
e2fsck -f -b 8193 /dev/<Defekte_Partition>
```

Die Option `-f` erzwingt den Dateisystem-Check und kommt damit dem möglichen Irrtum von `e2fsck` zuvor, es sei – angesichts der intakten Superblock-Kopie – alles in Ordnung.

10.5 Virtuelle Konsolen

Linux ist multitasking- und multiuserfähig. Auch wenn nur Sie selbst an Ihrem Rechner arbeiten, werden Sie die Vorteile, die diese Fähigkeiten mitbringen, zu schätzen lernen.

Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung, zwischen denen Sie über die Tastenkombinationen Alt + F1 bis Alt + F6 wechseln können. Die siebte Konsole ist für X11 reserviert, die achte für eine weitere X11-Sitzung. Durch Modifikation der Datei `/etc/inittab` können weitere oder weniger Konsolen zur Verfügung gestellt werden. Wenn Sie von X11 aus auf eine Textkonsole zurückschalten möchten, ohne X11 zu beenden, verwenden Sie Strg + Alt + F1 bis Strg + Alt + F6. Mit Alt + F7 kommen Sie zu X11 zurück.

10.6 Tastaturbelegung

Um die Tastaturbelegung von Programmen zu vereinheitlichen, wurden Änderungen an den folgenden Dateien vorgenommen:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Diese Änderungen wirken sich nur auf die Applikationen aus, die die `terminfo`-Einträge auslesen, bzw. deren Konfigurationsdateien direkt verändert wurden (`vi`, `less` etc.). Applikationen die nicht von SUSE stammen, sollten an diese Vorgaben angepasst werden.

Unter X ist die Compose-Taste (Multi_key) über die Tastenkombination Strg + Shift (rechts) zu erreichen. Beachten Sie dabei den entsprechenden Eintrag in `/usr/X11R6/lib/X11/Xmodmap`.

Zu Besonderheiten bei der Eingabe von Chinesich, Japanisch oder Koreanisch (CJK) finden Sie detaillierte Informationen auf Mike Fabians Seite: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

10.7 Lokale Anpassungen — I18N/L10N

SUSE LINUX ist internationalisiert und kann flexibel auf lokale Gegebenheiten abgestimmt werden. Die Internationalisierung (I18N) erlaubt spezielle Lokalisierungen (L10N). Die Abkürzungen I18N und L10N stehen für *internationalization* und *localization*: jeweils Anfangs- und Endbuchstabe und dazwischen die Anzahl der ausgelassenen Buchstaben.

Die Einstellungen werden über `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dabei geht es nicht nur um die Einstellung der Sprache für die Programmoberfläche und -meldungen (engl. *native language support*), sondern im Einzelnen um die Kategorien für *Nachrichten* (Sprache), *Zeichenklassen*, *Sortierreihenfolge*, *Datum und Uhrzeit*, *Zahlen* und *Geld*. Jede dieser Kategorien kann entweder gezielt über eine eigene Variable oder indirekt über eine übergeordnete Variable in der Datei `language` festgelegt werden (vgl. die Manualpage `man locale`).

1. `RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`: Diese Variablen werden ohne den `RC_`-Vorsatz an die Shell weitergereicht und bestimmen die oben genannten Kategorien; die betroffenen Dateien werden im Folgenden aufgezählt.

   Die aktuelle Einstellung kann mit dem Befehl `locale` abgefragt werden.

2. `RC_LC_ALL`: Diese Variable überschreibt, falls gesetzt, die Werte der in Punkt 1 genannten Variablen.

3. `RC_LANG`: Wenn keine der o. g. Variablen gesetzt ist, ist diese der Fallback. SUSE LINUX setzt standardmäßig nur `RC_LANG`; dadurch kann der Anwender leichter eigene Werte eintragen.

4. `ROOT_USES_LANG`: Eine `yes/no`-Variable. Ist sie auf `no` gesetzt, dann arbeitet `root` immer in der POSIX-Umgebung.

Die Variablen sind über den `sysconfig`-Editor zu setzen. Der Wert einer solchen Variablen setzt sich aus Sprachangabe (*language code*), Land oder Territorium (engl. *country code*), Zeichensatz (engl. *encoding*) und Option (engl. *modifier*) zusammen. Die einzelnen Angaben werden mit Spezialzeichen verbunden:

LANG=⟨*language*⟩[[_⟨*COUNTRY*⟩].⟨*Encoding*⟩[@⟨*Modifier*⟩]]

10.7.1 Einige Beispiele

Bitte setzen Sie die Sprach- und die Länderangabe immer zusammen. Die Angabe der Sprache folgt dem Standard ISO 639 (`http://www.evertype.com/standards/iso639/iso639-en.html` und `http://www.loc.gov/standards/iso639-2/`), die Ländercodes sind in ISO 3166 festgelegt (siehe `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`). Sinnvollerweise dürfen aber nur die Werte gewählt werden, für die verwendbare Beschreibungsdateien unter `/usr/lib/locale` zu finden sind. Weitere Beschreibungsdateien lassen sich mit Hilfe von `localedef` aus den Dateien in `/usr/share/i18n` erzeugen.

`LANG=de_DE.UTF-8` Dies ist die Standardeinstellung, wenn man in deutscher Sprache installiert; installiert man in einer anderen Sprache, wird auch UTF-8 als Zeichen-Kodierung gesetzt, aber die jeweils andere Sprache für das System eingestellt.

`LANG=de_DE.ISO-8859-1` So stellt man die deutsche Sprache in Deutschland mit Zeichensatz `ISO-8859-1` ein. Dieser Zeichensatz enthält nicht das Euro-Zeichen; man benötigt diesen Zeichensatz bisweilen noch, wenn ein Programm noch nicht an `UTF-8` angepasst ist.

Die Angabe des Zeichensatzes (hier `ISO-8859-1`) wertet zum Beispiel der Editor Emacs aus.

`LANG=de_DE@euro` Dies ist ein Beispiel für das Setzen einer Option (`euro`).

SuSEconfig liest die Variablen aus `/etc/sysconfig/language` aus und schreibt die Angaben nach `/etc/SuSEconfig/profile` und `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` wird von `/etc/profile` eingelesen (gesourcet) und `/etc/SuSEconfig/csh.cshrc` von `/etc/csh.cshrc`. Somit stehen die Einstellungen systemweit zur Verfügung.

Die Benutzer können die Systemvorgaben in `~/.bashrc` überschreiben. Wenn also die Systemvorgabe `de_DE` ist, kann der Benutzer, falls er mit deutschen Programmmeldungen nicht zufrieden ist, so auf englische Ausgaben umschalten: `LC_MESSAGES=en_US`.

10.7.2 Anpassung für Sprachunterstützung

Dateien der Kategorie *Nachrichten* werden in der Regel nur im Sprachverzeichnis (zum Beispiel `de`) abgelegt, um ein Fallback zu haben. Wenn

man also LANG auf de_AT setzt und die Message-Datei unter /usr/share/locale/de_AT/LC_MESSAGES nicht vorhanden ist, dann wird auf /usr/share/locale/de/LC_MESSAGES zurückgegriffen.

Auch kann man mit LANGUAGE eine Fallbackkaskade festlegen; zum Beispiel für bretonisch -> französisch oder für galizisch -> spanisch -> portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Oder um auf die norwegischen Variaten nynorsk bzw. bokmål auszuweichen (mit zusätzlichem Rückfall auf no):

```
LANG="nn_NO"
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"
LANGUAGE="nb_NO:nn_NO:no"
```

Bei Norwegisch ist auch zu beachten, dass LC_TIME unterschiedlich behandelt wird.

Mögliche Probleme

Der Tausenderpunkt wird nicht erkannt. Wahrscheinlich steht LANG beispielweise auf de. Da die Beschreibung, auf die die glibc zurückgreift, in /usr/share/lib/de_DE/LC_NUMERIC zu finden ist, muss beispielsweise LC_NUMERIC auf de_DE gesetzt werden.

Weitere Informationen:

- *The GNU C Library Reference Manual*, Kapitel „Locales and Internationalization“; enthalten im glibc-info.
- Jochen Hein, unter dem Stichwort „NLS“.
- *German-Howto* von Winfried Trümper file:/usr/share/doc/howto/en/html/German-HOWTO.html.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, aktuell unter http://www.cl.cam.ac.uk/~mgk25/unicode.html.
- *Unicode-Howto* von Bruno Haible file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html.
- *CJK Support in SuSE Linux* auf Englisch von Mike Fabian http://www.suse.de/~mfabian/suse-cjk/suse-cjk.html.

Das Bootkonzept

Das Booten und die Initialisierung eines Unix-Systems sind selbst für einem erfahrenen System-Administrator keineswegs trivial. Dieses Kapitel gibt eine kurze Einführung in das Bootkonzept von SUSE LINUX. Die vorliegende Implementierung der Systeminitialisierung setzt den Standard LSB in Version 1.3.x um (vgl. Abschnitt 10.1.1 auf Seite 268).

11.1 Das init-Programm 290
11.2 Die Runlevels 291
11.3 Wechsel des Runlevels 292
11.4 Die Init-Skripten 293
11.5 Der YaST Runlevel-Editor 297
11.6 SuSEconfig und /etc/sysconfig 299
11.7 Der YaST Sysconfig-Editor 301

Mit den lapidaren Worten „Uncompressing Linux...“ (bzw. bei IBM S/390 und zSeries nach dem IPL) übernimmt der Kernel die Kontrolle über die gesamte Hardware des Systems. Er prüft und setzt die Konsole — oder genauer: die BIOS-Register der Graphikkarte und das Ausgabeformat auf den Bildschirm —, um danach die Einstellungen im BIOS zu lesen und die elementaren Schnittstellen des Mainboards zu initialisieren. In den nächsten Schritten „proben“ die einzelnen Treiber — die ja Bestandteil des Kernels sind — die vorhandene Hardware, um sie gegebenenfalls zu initialisieren. Nach dem Überprüfen der Partitionen und dem Mounten des Root-Dateisystems startet der Kernel das Programm init. Durch init wird das eigentliche System „hochgefahren“ (Unix-Jargon) und die vielen Dienstprogramme und deren Konfiguration werden so gestartet. Der Kernel verwaltet dann das gesamte System; er überwacht Rechenzeit für die einzelnen Programme, er stellt Speicher zur Verfügung und steuert Hardware-Zugriffe.

11.1 Das init-Programm

Das Programm init ist der für die korrekte Initialisierung des Systems zuständige Prozess; alle Prozesse im System sind also „Kinder“ von init.

Unter allen Programmen nimmt init eine Sonderrolle ein: init wird direkt vom Kernel gestartet und ist immun gegen das Signal 9, mit dem normalerweise jeder Prozess „gekillt“ werden kann. Alle weiteren Prozesse werden entweder von init selbst oder von einem seiner „Kindprozesse“ gestartet.

Konfiguriert wird init zentral über die Datei `/etc/inittab`; hier werden die so genannten „Runlevels“ definiert (mehr dazu im Abschnitt 11.2 auf der nächsten Seite) und es wird festgelegt, welche Dienste und Daemonen in den einzelnen Levels zur Verfügung stehen sollen. Abhängig von den Einträgen in `/etc/inittab` ruft init verschiedene Skripten auf, die aus Gründen der Übersichtlichkeit im Verzeichnis `/etc/init.d/` zusammengefasst sind.

Der gesamte Hochlauf des Systems — und natürlich auch das Herunterfahren — wird somit einzig und allein vom init-Prozess gesteuert; insofern lässt sich der Kernel quasi als „Hintergrundprozess“ betrachten, dessen Aufgabe darin besteht, die gestarteten Prozesse zu verwalten, ihnen Rechenzeit zuzuteilen und den Zugriff auf die Hardware zu ermöglichen und zu kontrollieren.

11.2 Die Runlevels

Unter Linux existieren verschiedene *Runlevels*, die den jeweiligen Zustand des Systems definieren. Der Standard-Runlevel, in dem das System beim Booten hochfährt, ist in der Datei `/etc/inittab` durch den Eintrag `initdefault` festgelegt. Für gewöhnlich ist dies `3` oder `5` (siehe Überblick in Tabelle 11.1). Alternativ kann der gewünschte Runlevel beim Booten (zum Beispiel am Boot-Prompt) angegeben werden; der Kernel reicht die Parameter, die er nicht selbst auswertet, unverändert an den init-Prozess weiter.

Um zu einem späteren Zeitpunkt in einen anderen Runlevel zu wechseln, kann man init mit der Nummer des zugehörigen Runlevels aufrufen; das Wechseln des Runlevels kann nur vom Systemadministrator veranlasst werden. Beispielsweise gelangt man durch das Kommando `init 1` oder `shutdown now` in den Einzelbenutzerbetrieb (engl. *Single user mode*), der der Pflege und Administration des Systems dient. Nachdem der Systemadministrator seine Arbeit beendet hat, kann er durch `init 3` das System wieder in den normalen Runlevel hochfahren lassen, in dem alle für den Betrieb erforderlichen Programme laufen und sich die Benutzer beim System anmelden können. Mit `init 0` oder `shutdown -h now` kann das System angehalten, bzw. durch `init 6` oder `shutdown -r now` zu einem Neustart veranlasst werden.

Hinweis

Runlevel 2 bei NFS gemounteter /usr/ Partition

Runlevel 2 sollte auf einem System, dessen `/usr/` Partition via NFS gemountet ist, nicht verwendet werden. Die `/usr/` Partition enthält wichtige Programme, die zur reibungslosen Bedienbarkeit des Systems notwendig sind. Da der NFS-Dienst im Runlevel 2 (Lokaler Multiuserbetrieb ohne entferntes Netzwerk) noch nicht zur Verfügung steht, würde Ihr System in seiner Funktion stark beeinträchtigt.

Hinweis

Tabelle 11.1: *Liste der gültigen Runlevels unter Linux*

Runlevel	Bedeutung
0	Systemhalt (engl. *System halt*)
S	Einzelbenutzerbetrieb (engl. *Single user mode*); vom Bootprompt aus mit US-Tastaturbelegung

1	Einzelbenutzerbetrieb (engl. *Single user mode*)
2	Lokaler Multiuserbetrieb ohne entferntes Netzwerk (engl. *Local multiuser without remote network*) (d.h. NFS)
3	Voller Multiuserbetrieb mit Netzwerk (engl. *Full multiuser with network*)
4	Frei (engl. *Not used*)
5	Voller Multiuserbetrieb mit Netzwerk und KDM (Standard), GDM oder XDM (engl. *Full multiuser with network and xdm*)
6	Systemneustart (engl. *System reboot*)

Bei einer Standardinstallation von SUSE LINUX wird normalerweise Runlevel `5` als Standard eingerichtet, so dass sich die Benutzer direkt an der grafischen Oberfläche beim System anmelden können.

Wenn Sie den Runlevel von `3` auf `5` setzen wollen, muss sichergestellt sein, dass das X Window System bereits korrekt konfiguriert ist; (siehe Kapitel 12 auf Seite 305). Ob das System so wie von Ihnen gewünscht funktioniert, testen Sie danach durch Eingabe von `init 5`. Ist dies der Fall, können Sie den Standard-Runlevel über YaST auf `5` ändern.

Achtung

Eigene Änderungen an /etc/inittab

Eine fehlerhafte `/etc/inittab` kann dazu führen, dass das System nicht korrekt hochgefahren wird. Gehen Sie bei Veränderungen dieser Datei mit äußerster Sorgfalt vor und behalten Sie immer eine Kopie einer intakten Datei. Zur Behebung des Schadens können Sie versuchen, am Bootprompt den Parameter `init=/bin/sh` zu übergeben, um direkt in eine Shell zu booten und von dort aus die Datei wiederherzustellen. Nach dem Booten spielen Sie mittels `cp` die Backupkopie wieder ein.

Achtung

11.3 Wechsel des Runlevels

Generell passieren bei einem Wechsel des Runlevels folgende Dinge: Die *Stopp-Skripten* des gegenwärtigen Runlevels werden ausgeführt — dabei

werden typischerweise verschiedene, in diesem Level laufende Programme beendet — und die *Start-Skripten* des neuen Runlevels werden ausgeführt. Während eines solchen Vorgangs werden in den meisten Fällen einige Programme gestartet.

Um dies zu verdeutlichen, betrachten wir an einem Beispiel den Wechsel von Runlevel 3 nach Runlevel 5:

- Der Administrator (`root`) teilt dem init-Prozess mit, dass der Runlevel gewechselt werden soll. In diesem Fall erreicht er dies durch Eingabe von `init 5`.
- init konsultiert die Konfigurationsdatei `/etc/inittab` und stellt fest, dass das Skript `/etc/init.d/rc` mit dem neuen Runlevel als Parameter aufgerufen werden muss.
- Nun ruft rc alle Stopp-Skripten des gegenwärtigen Runlevels auf, für die im neuen Runlevel kein Start-Skript existiert; in unserem Beispiel sind das alle Skripten, die sich im Verzeichnis `/etc/init.d/rc3.d/` befinden (der alte Runlevel war `3`) und mit einem `K` beginnen. Die nach dem `K` folgende Zahl gewährleistet, dass hierbei eine bestimmte Reihenfolge eingehalten wird, da unter Umständen manche Programme von anderen abhängig sind.
- Als Letztes werden die Start-Skripten des neuen Runlevels aufgerufen; diese liegen in unserem Beispiel unter `/etc/init.d/rc5.d/` und beginnen mit einem `S`. Auch hierbei wird eine bestimmte Reihenfolge eingehalten, die durch die dem `S` folgende Zahl festgelegt ist.

Wenn Sie in denselben Runlevel wechseln, in dem Sie sich bereits befinden, liest init nur die `/etc/inittab` ein, prüft sie auf Veränderungen und nimmt bei Bedarf die entsprechenden Maßnahmen vor, etwa das Starten eines `getty` auf einer weiteren Schnittstelle.

11.4 Die Init-Skripten

Die Skripten unter `/etc/init.d/` unterteilen sich in zwei Kategorien:

- Skripte, die *direkt* von init aufgerufen werden: Dies ist nur beim Booten der Fall sowie bei einem sofortigen Herunterfahren des Systems

(bei Stromausfall oder durch Drücken der Tastenkombination Strg + Alt + Entf durch den Anwender). Bei IBM S/390 und zSeries tritt dieser Fall nur beim Booten sowie bei einem sofortigen Herunterfahren des Systems (bei Stromausfall oder per „signal quiesce“) auf.

- Skripte, die *indirekt* von init aufgerufen werden: Das geschieht bei einem Wechsel des Runlevels; es wird generell das übergeordnete Skript /etc/init.d/rc ausgeführt, das dafür sorgt, dass die relevanten Skripten in der korrekten Reihenfolge aufgerufen werden.

Alle Skripten befinden sich unter `/etc/init.d/`. Die Skripten für das Wechseln des Runlevels befinden sich ebenfalls in diesem Verzeichnis, werden jedoch grundsätzlich als symbolischer Link aus einem der Unterverzeichnisse `/etc/init.d/rc0.d/` bis `/etc/init.d/rc6.d/` aufgerufen. Dies dient der Übersichtlichkeit und vermeidet, dass Skripten mehrfach vorhanden sein müssen, etwa weil sie in verschiedenen Runlevels verwendet werden sollen. Da jedes dieser Skripten sowohl als Start- wie auch als Stopp-Skript aufgerufen werden kann, müssen sie alle die beiden möglichen Parameter `start` und `stop` verstehen. Zusätzlich verstehen die Skripten die Optionen `restart`, `reload`, `force-reload` und `status`; die Bedeutung aller Optionen ist in Tabelle 11.2 aufgelistet.

Tabelle 11.2: *Übersicht der Optionen der init-Skripten*

Option	Bedeutung
`start`	Dienst starten
`stop`	Dienst stoppen
`restart`	Dienst stoppen und erneut starten, wenn der Dienst bereits lief; andernfalls den Dienst starten
`reload`	Konfiguration des Dienstes erneut einlesen, ohne den Dienst zu stoppen und neu zu starten
`force-reload`	Konfiguration des Dienstes erneut einlesen, wenn der Dienst dies unterstützt; andernfalls wie `restart`
`status`	aktuellen Status anzeigen

Die Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen dienen somit also nur dazu, eine Zuordnung der einzelnen Skripten zu bestimmten Runlevels zu ermöglichen. Das Anlegen und Entfernen der not-

wendigen Links geschieht mit insserv (bzw. dem Link `/usr/lib/lsb/install_initd`) beim Installieren oder Deinstallieren des jeweiligen Paketes; vgl. die Manualpage von insserv.

Im Folgenden finden Sie eine kurze Beschreibung der ersten Boot- und der letzten Shutdown-Skripten sowie des Steuerskripts:

`boot` Wird beim Start des Systems ausgeführt und direkt von init gestartet. Es ist unabhängig vom gewünschten Default-Runlevel und wird nur genau ein einziges Mal ausgeführt: Im Wesentlichen werden `proc`- und `pts`-Dateisystem eingehängt („gemountet"), der blogd (engl. *Boot Logging Daemon*) wird aktiviert und — nach einer Erstinstallation oder einem Update des Systems — wird eine Grundkonfiguration angestoßen.

Der blogd Daemon ist ein Daemon, der vom boot *und* rc Skript vor allem anderen gestartet wird und nach getaner Arbeit (zum Beispiel dem Aufruf von Unterskripten) wieder beendet wird. Dieser Daemon schreibt in die Log-Datei `/var/log/boot.msg`, falls `/var/` les- und schreibbar gemountet ist bzw. puffert alle Bildschirmdaten bis das `/var/` les- und schreibbar gemountet wird. Weitere Informationen zu blogd finden Sie unter `man blogd`.

Diesem Skript ist des Weiteren das Verzeichnis `/etc/init.d/boot.d/` zugeordnet; alle in diesem Verzeichnis gefundenen Skripte, die mit `S` beginnen, werden automatisch beim Hochlauf des Systems ausgeführt. Es werden die Dateisysteme geprüft, etwaige überflüssige Dateien unter `/var/lock/` gelöscht und das Netzwerk für das Loopback-Device konfiguriert, sofern dies vorgesehen ist. Weiterhin wird die Systemzeit gesetzt.

Tritt beim Prüfen und automatischen Reparieren der Dateisysteme ein schwerer Fehler auf, hat der Systemadministrator nach Eingabe des Root-Passwortes die Möglichkeit, manuell eine Lösung des Problems herbeizuführen. Schließlich wird das Skript boot.local ausgeführt.

`boot.local` Hier können weitere Dinge eingetragen werden, die beim Start geschehen sollen, bevor das System in einen der Runlevels eintritt; es kann von seiner Funktion her mit der vielleicht von DOS her gewohnten `AUTOEXEC.BAT` verglichen werden.

`boot.setup` Grundlegende Einstellungen, die beim Übergang vom Einzelnutzerbetrieb in irgendeinen Runlevel vorgenommen werden müssen. Hier werden die Tastaturbelegung und die Konsolenkonfiguration geladen.

halt Dieses Skript wird nur beim Eintritt in den Runlevel 0 oder 6 ausgeführt. Dabei wird es entweder unter dem Namen `halt` oder dem Namen `reboot` aufgerufen. Abhängig davon, wie halt aufgerufen wurde, wird das System neu gestartet oder ganz heruntergefahren.

rc Das übergeordnete Skript, das bei jedem Wechsel des Runlevels aufgerufen wird. Es führt die Stopp-Skripten des gegenwärtigen Runlevels aus und danach die Start-Skripten des neuen.

11.4.1 Init-Skripten hinzufügen

Zusätzliche Init-Skripten lassen sich in das oben beschriebene Konzept leicht integrieren. Orientieren Sie sich bei Fragen zum Format, Namensgebung und Organisation der Init-Skripten an den Vorgaben des LSB und den Manualpages von `init`, `init.d/` und `insserv`. Hilfreich sind in diesem Zusammenhang weiterhin die Manualpages von `startproc` und `killproc`.

Achtung

Erstellung eigener Init-Skripten

Fehlerhafte Init-Skripten können das gesamte System „aufhängen“. Erstellen Sie eigene Skripte mit äußerster Sorgfalt und testen Sie sie — soweit möglich — vor dem Ernstfall in der Multiuserumgebung. Grundlageninformation zum Umgang mit Runleveln/Init-Skripten finden Sie im Abschnitt 11.2 auf Seite 291.

Achtung

Wenn Sie für ein eigenes Programm oder eigenen Dienst (engl. *service*) ein Init-Skript erstellen, verwenden Sie die Datei `/etc/init.d/skeleton` als Vorlage. Speichern Sie diese Datei unter dem neuen Namen und editieren Sie die Nennung von Programm- oder Dateinamen und Pfaden und fügen Sie, wenn nötig, eigene Skriptbestandteile hinzu, die für ein korrektes Ausführen des Init-Aufrufes benötigt werden.

Editieren Sie den obligatorischen `INIT INFO` Block am Anfang der Datei:

Beispiel 11.1: *Eine minimale INIT INFO*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
```

```
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

In der ersten Zeile des `INFO`-Headers nennen Sie nach `Provides:` den Namen des Programms oder Dienstes, der mit diesem Init-Skript gesteuert werden soll. `Required-Start:` und `Required-Stop:` enthalten alle Dienste, die vor dem Start oder Stopp des betroffenen Dienstes oder Programms gestartet oder gestoppt werden müssen. Diese Information wird ausgewertet, um die Numerierung der resultierenden Start- und Stoppskripten in den Runlevel-Verzeichnissen zu generieren. Die Runlevel, in denen Ihre Anwendung automatisch gestartet bzw. gestoppt werden sollen, geben Sie bei `Default-Start:` und `Default-Stop:` an. Mit einer kurzen Beschreibung Ihrer Anwendung unter `Description:` schließen Sie Ihre Eingaben ab.

Legen Sie mit dem Befehl `insserv <Name des neuen Skripts>` die Links von `/etc/init.d/` in die entsprechenden Runlevelverzeichnisse (`/etc/init.d/rc?.d/)/` an. insserv wertet automatisch die im Header des Init-Skripts gemachten Angaben aus und legt die Links für Start- und Stoppskripte in den entsprechenden Runlevelverzeichnissen ab. Die korrekte Start- und Stoppreihenfolge innerhalb eines Runlevels wird ebenfalls über die Nummerierung der Skripte von insserv gewährleistet. Als grafisches Konfigurationswerkzeug zum Anlegen der Links steht der Runlevel-Editor von YaST zur Verfügung; vgl. Abschnitt 11.5.

Soll lediglich ein in `/etc/init.d/` bereits vorliegendes Skript in das Runlevel-Konzept eingebunden werden, legen Sie mittels insserv oder dem YaST-Runlevel-Editor die Links in die entsprechenden Runlevelverzeichnisse an und aktivieren den Dienst. Beim nächsten Start des Systems werden Ihre Änderungen umgesetzt und der neue Dienst automatisch gestartet.

11.5 Der YaST Runlevel-Editor

Nach dem Start dieses Moduls gelangen Sie in eine Übersichtsmaske, die alle verfügbaren Dienste und deren Aktivierungszustand wiedergibt. Entscheiden Sie sich per Radiobutton für einen der beiden Modi ‘Einfacher

Modus' oder 'Expertenmodus'. Voreingestellt und für die meisten Anwendungssituationen ausreichend ist der 'Einfache Modus'. In einer tabellarischen Übersicht sind alphabetisch geordnet alle Dienste und Daemonen aufgelistet, die auf Ihrem System zur Verfügung stehen. In der linken Spalte stehen die Namen der Dienste, in der Mitte ihr Aktivierungszustand und in der rechten Spalte eine kurze Beschreibung. Unterhalb der Übersicht wird zum aktuell selektierten Dienst eine ausführlichere Beschreibung eingeblendet. Um einen Dienst zu aktivieren, selektieren Sie ihn in der Übersicht und klicken auf 'Aktivieren'. Entsprechend gehen Sie vor, um aktive Dienste zu deaktivieren.

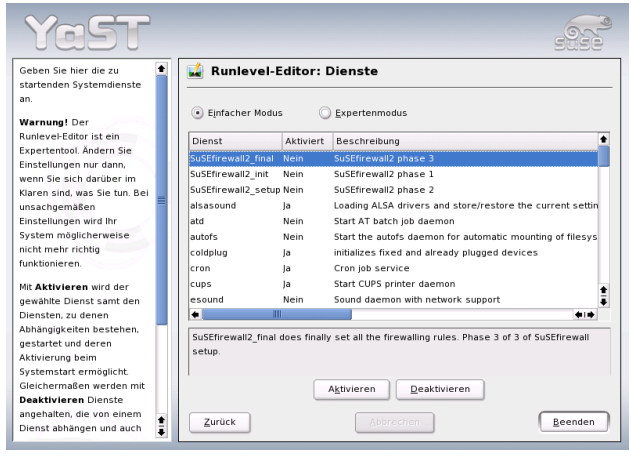

Abbildung 11.1: *YaST Runlevel-Editor*

Möchten Sie gezielt den Runlevel beeinflussen, in dem ein Dienst gestartet oder gestoppt werden soll oder den Standard-Runlevel verändern, wechseln Sie per Radiobutton in den 'Expertenmodus'. In dieser Maske wird zuerst der aktuelle Standard-Runlevel angezeigt. Dieser „Betriebsmodus" wird nach dem Booten Ihres Systems hochgefahren. Bei SUSE LINUX ist dies üblicherweise Runlevel 5 (voller Multiuserbetrieb mit Netzwerk und XDM). Geeignet wäre zum Beispiel auch Runlevel 3 (voller Multiuserbetrieb mit Netzwerk). An dieser Stelle lässt sich mit Hilfe von YaST ein anderer Default-Runlevel einstellen; vgl. Tabelle 11.1 auf Seite 291. Die De-/Aktivierung von Diensten und Daemonen geschieht über die tabellarische Übersicht. Sie erhalten dort Information darüber, welche Dienste und Daemonen vorhanden sind, ob diese in Ihrem System aktiv geschaltet sind und

für welche Runlevels dies gilt. Wenn Sie eine Zeile per Mausklick markieren, haben Sie die Möglichkeit, die Checkboxen für die Runlevels 'B', '0', '1', '2', '3', '5', '6' und 'S' zu aktivieren und damit festzulegen, für welche Runlevels der entsprechende Dienst bzw. Daemon aktiv werden soll. Runlevel 4 ist nicht definiert — dieser ist stets frei für benutzereigene Einstellungen. Unmittelbar unterhalb der Übersicht wird eine kurze Beschreibung des jeweils selektierten Dienstes oder Daemons angezeigt.

Mit 'Starten/Anhalten/Aktualisieren' entscheiden Sie, ob ein Dienst eingesetzt werden soll. Mit 'Status aktualisieren' sind Sie in der Lage, den aktuellen Status zu prüfen, falls dies nicht automatisch geschieht. Über 'Anwenden/Zurücksetzen' selektieren Sie, ob der von Ihnen konfigurierte Zustand übernommen werden soll oder der Ausgangszustand vor Aufruf des Runlevel-Editors wiederhergestellt werden soll. Mit 'Beenden' speichern Sie die Systemkonfiguration.

Achtung

Editieren der Runlevel-Einstellungen

Fehlerhafte Einstellungen von Systemdiensten und Runleveln können Ihr System unbrauchbar machen. Informieren Sie sich vor einer Änderung dieser Einstellungen über die möglichen Folgen, um die Funktionsfähigkeit Ihres Systems zu gewährleisten.

Achtung

11.6 SuSEconfig und /etc/sysconfig

Die wesentliche Konfiguration von SUSE LINUX nehmen Sie über die Konfigurationsdateien unter `/etc/sysconfig/` vor. Frühere Versionen von SUSE LINUX verwendeten zur Systemkonfiguration die Datei `/etc/rc.config/`, die mittlerweile obsolet wurde. Bei einer Neuinstallation von SUSE LINUX wird diese Datei nicht mehr angelegt. Sämtliche Systemkonfiguration wird über die Dateien unter `/etc/sysconfig/` vorgenommen. Bei einem Update bleibt eine bestehende `/etc/rc.config/` jedoch erhalten.

Auf die Dateien in `/etc/sysconfig/` wird nur gezielt von einzelnen Skripten zugegriffen; dadurch wird gewährleistet, dass zum Beispiel die Netzwerkeinstellungen auch nur von dem Netzwerk-Skripten ausgewertet werden müssen. Darüber hinaus werden viele weitere Konfigurationsdateien des Systems in Abhängigkeit von den Dateien in `/etc/sysconfig/`

generiert; diese Aufgabe erledigt SuSEconfig. So wird beispielsweise nach einer Änderung der Netzwerkkonfiguration die Datei `/etc/host.conf` neu erzeugt, da sie abhängig von der Art der Konfiguration ist.

Wenn Sie Änderungen an den genannten Dateien vornehmen, müssen Sie nachfolgend immer SuSEconfig aufrufen, so dass die neuen Einstellungen auch an allen relevanten Stellen wirksam werden. Verändern Sie die Konfiguration mit dem YaST Sysconfig-Editor, brauchen Sie sich darum nicht explizit zu kümmern; YaST startet automatisch SuSEconfig, wodurch die betroffenen Dateien auf den aktuellen Stand gebracht werden.

Dieses Konzept ermöglicht es, grundlegende Änderungen an der Konfiguration des Rechners vornehmen zu können, ohne die Maschine neu booten zu müssen. Da manche Einstellungen sehr tief greifend sind, müssen jedoch unter Umständen einige Programme neu gestartet werden, um die Änderungen wirksam werden zu lassen.

Wenn Sie zum Beispiel Änderungen an der Netzwerkkonfiguration vorgenommen haben, erreichen Sie durch manuelles Ausführen der Kommandos `rcnetwork stop` und `rcnetwork start`, dass die betroffenen Netzwerk-Programme neu gestartet werden.

Für das Konfigurieren des Systems ist folgender Weg zu empfehlen:

- Bringen Sie das System durch Eingabe von `init 1` in den *single user mode* (Runlevel 1).
- Nehmen Sie die gewünschten Änderungen an den Konfigurationsdateien vor. Dies entweder kann mit einem Texteditor geschehen oder besser mit dem Sysconfig-Editor von YaST; vgl. in Abschnitt 11.7 auf der nächsten Seite.

Achtung

Manuelles Editieren der Systemkonfiguration

Wenn Sie die Konfigurationsdateien in `/etc/sysconfig/` *nicht* mit YaST bearbeiten, achten Sie darauf, dass Sie einen leeren Parameter als zwei aufeinander folgende Anführungszeichen schreiben (zum Beispiel `KEYTABLE=""`) und Parameter, die Leerzeichen enthalten, in Anführungsstriche einschließen. Bei Variablen, die nur aus einem Wort bestehen, sind die Anführungszeichen nicht notwendig.

Achtung

- Führen Sie SuSEconfig aus, um die Änderungen in die verschiedenen weiteren Konfigurationsdateien eintragen zu lassen. Dies geschieht automatisch, wenn Sie YaST verwendet haben, um den Runlevel zu setzen.
- Bringen Sie das System durch Eingabe von `init 3` in den vorherigen Runlevel zurück (hier im Beispiel `3`).

Diese Vorgehensweise ist natürlich nur bei sehr weitreichenden Änderungen an den Einstellungen des Systems erforderlich (zum Beispiel Netzwerkkonfiguration); bei einfachen Aufgaben ist es nicht erforderlich, für die Administration in den „single user mode“ zu wechseln; jedoch stellen Sie damit sicher, dass auch wirklich alle von der Änderung betroffenen Programme neu gestartet werden.

Hinweis

Sie können die automatische Konfiguration via SuSEconfig *global* abschalten, indem Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/suseconfig` auf `no` setzen. Wollen Sie den Installationssupport in Anspruch nehmen, muss `ENABLE_SUSECONFIG` allerdings auf `yes` gesetzt sein. Einzelne Teile der Autokonfiguration können auch gezielt deaktiviert werden.

Hinweis

11.7 Der YaST Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig/` sind die Dateien mit den wichtigsten Einstellungen für SUSE LINUX hinterlegt. Der YaST Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und anschließend in die einzelnen Konfigurationsdateien übernommen werden. Im Allgemeinen ist das manuelle Editieren allerdings nicht notwendig, da bei der Installation eines Paketes oder beim Einrichten eines Dienstes etc. die Dateien automatisch angepasst werden.

Achtung

Änderungen in den /etc/sysconfig/*-Dateien

Ihre Änderungen in `/etc/sysconfig/*/` haben tief greifende Folgen für Ihr gesamtes System. Bitte informieren Sie sich vor jeder Änderung ausreichend über die möglichen Folgen. So stellen Sie sicher, dass Ihr System funktionsfähig bleibt. Sämtliche Sysconfig-Variablen in den `/etc/sysconfig/`-Dateien sind mit kurzen Kommentaren versehen, die die Funktion der jeweiligen Variablen dokumentieren.

Achtung

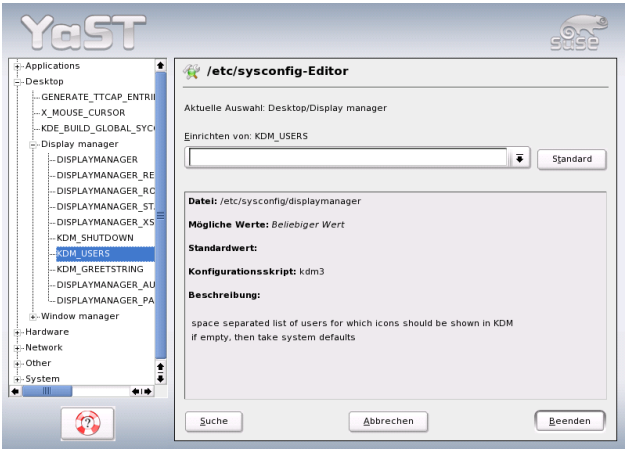

Abbildung 11.2: *YaST: Systemkonfiguration mit dem Sysconfig-Editor*

Der YaST Sysconfig-Editor startet mit einer in drei Teilbereiche gegliederten Maske. Im linken Teil der Maske können Sie in einer Baumansicht die zu konfigurierende Variable selektieren. Sobald Sie eine Variable selektieren, erscheint in der rechten Fensterhälfte die Bezeichnung der Selektion und die derzeit aktive Einstellung der Variablen. Unterhalb der Variablen wird eine kurze Beschreibung, möglichen Werte, die Standardeinstellung, sowie die Datei, in der diese Variable gespeichert wird, angezeigt. Weiterhin wird in dieser Maske angezeigt, welches Konfigurationsskript bei Änderung dieser Variablen ausgeführt wird und welcher Dienst neu gestartet wird. YaST bittet Sie um eine Bestätigung der Änderungen und informiert Sie,

welche Skripte im Anschluss an ein Verlassen des Moduls mit ‘Beenden’ ausgeführt werden sollen. Sie haben die Möglichkeit, das Starten bestimmter Dienste und Skripte zu überspringen, wenn Sie sie an dieser Stelle noch nicht starten wollen.

Das X Window System

Das X Window System (X11) ist der Quasi-Standard für grafische Benutzeroberflächen unter Unix. X11 ist zudem netzwerkbasiert, sodass Anwendungen, die auf einem Rechner gestartet wurden ihre Ausgabe auf einem anderen Rechner darstellen können, wenn beide miteinander vernetzt sind. Die Art des Netzes (LAN oder Internet) spielt hierbei keine Rolle.

Wir stellen Ihnen in diesem Kapitel Optimierungsmöglichkeiten für Ihre X Window System-Umgebung vor, geben Ihnen Hintergrundinformationen zum Umgang mit Fonts unter SUSE LINUX und gehen auf die OpenGL/3D-Konfiguration ein. Die YaST Modulbeschreibungen zur Konfiguration von Monitor, Grafikkarte, Maus und Tastatur finden Sie Installationsteil dieses Handbuches (Abschnitt 2.4.5 auf Seite 81).

► **S/390, zSeries**
Dieses Kapitel ist auf S/390 und zSeries Installationen von SUSE LINUX Enterprise Server nicht anwendbar, da bei diesen Geräten kein Display existiert, das von XFree unterstützt wird. ◄

12.1 Installation des X Window Systems optimieren . . 306
12.2 Installation und Konfiguration von Fonts 312
12.3 Konfiguration von OpenGL/3D 318

12.1 Installation des X Window Systems optimieren

Um die zur Verfügung stehende Hardware (Maus, Grafikkarte, Monitor, Tastatur) optimal nutzen zu können, besteht die Möglichkeit, die Konfiguration manuell zu optimieren. Im Folgenden wird auf einige Aspekte der Optimierung eingegangen. Detaillierte Informationen zur Konfiguration des X Window System finden sich in verschiedenen Dateien im Verzeichnis `/usr/share/doc/packages/xf86` sowie natürlich in der Manpage `man XF86Config`.

Achtung

Bei der Konfiguration des X Window Systems sollte besonders sorgsam vorgegangen werden! Auf keinen Fall sollte X11 gestartet werden, bevor die Konfiguration abgeschlossen wurde. Ein falsch eingestelltes System kann zu irreparablen Schäden an der Hardware führen; besonders gefährdet sind Festfrequenz-Monitore. Die Autoren dieses Buches und die SUSE LINUX AG lehnen jede Verantwortung für eventuell entstehende Schäden ab. Der vorliegende Text wurde mit größtmöglicher Sorgfalt erstellt. Dennoch kann nicht garantiert werden, dass die hier vorgestellten Methoden korrekt sind und Ihrer Hardware keinen Schaden zufügen.

Achtung

Die Programme SaX2 und xf86config erstellen die Datei `XF86Config`, standardmäßig in `/etc/X11`. Dies ist die primäre Konfigurationsdatei für das X Window System. Hier finden sich die gemachten Angaben zu Maus, Monitor und Grafikkarte.

Im Folgenden soll der Aufbau der Konfigurationsdatei `/etc/X11/XF86Config` vorgestellt werden. Diese Datei ist in Abschnitte (engl. *Sections*) aufgeteilt, die jeweils mit dem Schlüsselwort `Section "bezeichner"` eingeleitet werden und mit `EndSection` beendet werden. Es folgt ein grober Abriss der wichtigsten Abschnitte.

`XF86Config` setzt sich aus mehreren Abschnitten zusammen (den sog. Sections), die sich mit jeweils einem Aspekt der Konfiguration beschäftigen. Eine Section hat stets die Form:

```
Section Abschnittsbezeichnung
eintrag 1
```

```
eintrag 2
eintrag n
EndSection
```

Es existieren folgende Typen von Sections:

Tabelle 12.1: *Abschnitte (sog. sections) in /etc/X11/XF86Config*

Typ	Bedeutung
`Files`	Dieser Abschnitt beschreibt die verwendeten Pfade für Zeichensätze und die RGB-Farbtabelle.
`ServerFlags`	Hier werden allgemeine Schalter angegeben.
`InputDevice`	Über diesen Abschnitt werden die Eingabegeräte konfiguriert. Es werden sowohl Tastaturen und Mäuse als auch spezielle Eingabegeräte (Touchtablett, Joysticks usw.) über diesen Abschnitt konfiguriert. Wichtige Bezeichner sind hier `Driver` und die Optionen, die `Protocol` und `Device` festlegen.
`Monitor`	Beschreibt den verwendeten Monitor. Elemente dieses Abschnittes sind ein Name, auf den später bei der Definition des `Screens` verwiesen wird, sowie die Beschreibung der Bandbreite (`Bandwidth`) und der zulässigen Synchronisationsfrequenzen (`HorizSync` und `VertRefresh`). Die Angaben erfolgen in MHz, kHz bzw. Hz. Grundsätzlich lehnt der Server jede Modeline ab, die nicht der Spezifikation des Monitors entspricht. Damit soll verhindert werden, dass durch Experimente an den Modelines versehentlich zu hohe Frequenzen an den Monitor geschickt werden.
`Modes`	Hier werden die Darstellungsparameter der einzelnen Bildschirmauflösungen festgelegt. Diese Parameter können von SaX2 aufgrund der vom Benutzer vorgegebenen Werte berechnet werden und müssen im Regelfall nicht verändert werden. Manuell eingreifen können Sie an dieser Stelle aber beispielsweise, wenn Sie einen Festfrequenzbildschirm anschließen möchten. Eine genaue Erläuterung der einzelnen Parameter würde den Rahmen dieses Buches sprengen, Sie finden allerdings eine detaillierte Erläuterung der Bedeutung der einzelnen Zahlenwerte in der HOWTO Datei `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.

`Device`	Dieser Abschnitt definiert eine bestimmte Grafikkarte. Diese wird durch den angegeben Namen referenziert.
`Screen`	Diese Section schließlich fügt einen `Monitor` und ein `Device` zusammen und es ergeben sich daraus die notwendigen Angaben für XFree. Der Unterabschnitt `Display` erlaubt die Angabe der virtuellen Bildschirmgröße (`Virtual`), des `ViewPort` und der verwendeten `Modes` mit diesem Screen.
`ServerLayout`	Dieser Abschnitt legt das Layout einer Single- oder Multiheadkonfiguration fest. Hier werden die Eingabegeräte `InputDevice` und die Anzeigegeräte `Screen` zu einem Ganzen zusammengefasst.

Näher betrachtet werden die Sections `Monitor`, `Device` und `Screen`. In der Manualpage von `XFree86` und der Manualpage von `XF86Config` finden sich weitere Informationen zu den verbleibenden Sections.

In `XF86Config` können mehrere `Monitor`- und `Device`-Abschnitte vorkommen. Auch mehrere `Screen`-Abschnitte sind möglich; welcher davon verwendet wird, hängt dann vom nachfolgenden Abschnitt `ServerLayout` ab.

12.1.1 Screen-Section

Zunächst soll die Screen-Section näher betrachtet werden. Diese bringt eine Monitor- mit einer Device-Section zusammen und bestimmt, welche Auflösungen mit welcher Farbtiefe bereitgestellt werden sollen.

Eine Screen-Section kann beispielsweise wie in Datei 12.1 aussehen.

Beispiel 12.1: *Die Screen-Section der Datei /etc/X11/XF86Config*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
```

```
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

Die Zeile `Identifier` (hier `Screen[0]`) gibt diesem Abschnitt eine eindeutige Bezeichnung, durch die er dann im darauf folgenden Abschnitt `ServerLayout` eindeutig referenziert werden kann. Über die Zeilen `Device` und `Monitor` werden dem `Screen` eindeutig die schon weiter oben in der Datei definierte Grafikkarte und der Monitor zugeordnet. Dies sind nichts weiter als Verweise auf die Device- und Monitor-Sections mit den entsprechenden Namen bzw. Identifiern. Auf diese Sections wird weiter unten noch näher eingegangen.

Mittels der `DefaultDepth`-Angabe kann ausgewählt werden, in welcher Farbtiefe der Server startet, wenn er ohne eine explizite Angabe der Farbtiefe gestartet wird. Es folgt für jede Farbtiefe eine `Display`-Subsection. Die Farbtiefe, für die die Subsection gilt, wird durch das Schlüsselwort `Depth` festgelegt. Mögliche Werte für `Depth` sind 8, 15, 16 und 24. Nicht alle X-Server-Module unterstützen jeden dieser Werte.

Nach der Farbtiefe wird mit `Modes` eine Liste von Auflösungen festgelegt. Diese Liste wird vom X-Server von links nach rechts durchlaufen. Für jede Auflösung wird in der Modes-Section in Abhängigkeit von der Monitor-Section eine passende `Modeline` gesucht, die vom Monitor und der Grafikkarte dargestellt werden kann.

Die erste in diesem Sinne passende Auflösung ist die, in der der X-Server startet (der sog. `Default-Mode`). Mit den Tasten Strg-Alt-Grau + kann in der Liste nach rechts, mit Strg-Alt-Grau - nach Links gewandert werden. So kann die Bildschirmauflösung zur Laufzeit des X Window Systems variiert werden.

Die letzte Zeile der Subsection `Display` mit `Depth 16` bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe des virtuellen Bildschirms hängt vom Speicherausbau der Videokarte und der

gewünschten Farbtiefe ab, nicht aber von der maximalen Auflösung des Monitors. Da moderne Grafikkarten sehr viel Grafikspeicher anbieten, können Sie sehr große virtuelle Desktops anlegen. Beachten Sie dann aber bitte, dass Sie evtl. keine 3D-Funktionalität mehr nutzen können, wenn Sie praktisch den gesamten Grafikspeicher mit einem virtuellen Desktop füllen. Hat die Karte zum Beispiel 16 MB Video-RAM, so kann, bei 8 Bit Farbtiefe, der virtuelle Bildschirm bis zu 4096x4096(!) Pixel groß sein. Speziell bei den beschleunigten Servern empfiehlt es sich jedoch nachdrücklich, nicht den gesamten Speicher der Videokarte für den virtuellen Bildschirm zu verwenden, da der nicht verwendete Speicherbereich auf der Videokarte von diesen Servern für verschiedene Caches für Zeichensätze und Grafikbereiche verwendet wird.

12.1.2 Device-Section

Eine Device-Section beschreibt eine bestimmte Grafikkarte. Es können beliebig viele Device-Sections in `XF86Config` enthalten sein, solange sich ihr Name, der mit dem Schlüsselwort `Identifier` angegeben wird, unterscheidet. In der Regel werden – falls Sie mehrere Grafikkarten eingebaut haben – die Sections einfach durchnummeriert, die erste wird dann mit `Device[0]`, die zweite mit `Device[1]` bezeichnet usw.. In der folgenden Datei sehen Sie den Ausschnitt aus der `Device` Section eines Computers, in dem eine Matrox Millennium PCI Grafikkarte eingebaut ist:

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Wenn Sie SaX2 zur Konfiguration verwenden, dann dürfte die Device-Section ungefähr so wie oben abgebildet aussehen. Insbesondere `Driver` und `BusID` sind natürlich von der in Ihrem Computer eingebauten Hardware abhängig und werden von SaX2 automatisch bestimmt. Die `BusID` bestimmt den PCI- bzw. AGP-Steckplatz, in den die Grafikkarte eingesteckt ist. Diese stimmt mit der vom Kommando lspci ausgegebenen ID überein. Beachten Sie, dass der X-Server die Angaben in dezimaler, das Programm lspci hingegen in hexadezimaler Schreibweise ausgibt!

Über den Parameter `Driver` legen Sie den zu verwendenden Treiber für diese Grafikkarte fest. Im Falle der Matrox Millennium heißt das Treibermodul `mga`. Diese werden vom X-Server über den im Abschnitt `Files` definierten `ModulePath` im Unterverzeichnis `drivers` gesucht. In einer Standardinstallation ist dies das Verzeichnis `/usr/X11R6/lib/modules/drivers`. Hierzu wird an den Namen einfach `_drv.o` angehängt, im Falle des `mga` Treibers wird die Treiberdatei `mga_drv.o` geladen.

Über zusätzliche Optionen kann das Verhalten des X-Servers bzw. des Treibers beeinflusst werden. In der Device Section ist hier exemplarisch die Option `sw_cursor` gesetzt worden. Dies deaktiviert den Hardwaremauscursor und stellt den Mauszeiger in Software dar. Je nach Treibermodul stehen ihnen verschiedene Optionen zur Verfügung, diese sind in den Beschreibungsdateien zu den Treibermodulen im Verzeichnis `/usr/X11R6/lib/X11/doc` zu finden. Allgemein gültige Optionen finden Sie auch in den Manpages (`man XF86Config` und `man XFree86`).

12.1.3 Monitor- und Modes-Section

Die Monitor-Sections und die Modes-Section beschreiben, analog zu den Device-Sections, jeweils einen Monitor. Die Konfigurationsdatei `/etc/X11/XF86Config` kann wieder beliebig viele, unterschiedlich benannte Monitor-Sections enthalten. In der ServerLayout-Section wird dann festgelegt, welche Monitor-Section ausschlaggebend ist.

Für die Monitordefinition gilt, noch mehr als für die Beschreibung der Grafikkarte, dass das Erstellen einer Monitor-Section und insbesondere der Modes-Section nur von erfahrenen Benutzern gemacht werden sollte. Der wesentliche Bestandteil der Modes-Section sind die so genannten Modelines, in denen Horizontal- und Vertikal-Timings für die jeweilige Auflösung angegeben werden. In der Monitor-Section werden die Eigenschaften des Monitors, insbesondere die zulässigen Ablenkfrequenzen, festgehalten.

Achtung

Ohne ein grundlegendes Verständnis der Funktionsweise von Monitor und Grafikkarte sollte an den Modelines nichts verändert werden, da dies unter Umständen zur Zerstörung des Monitors führen kann!

Achtung

Wer sich zutraut, eigene Monitorbeschreibungen zu entwickeln, sollte mit der Dokumentation im Verzeichnis `/usr/X11/lib/X11/doc` vertraut

sein. Besonders zu erwähnen ist [20], wo die Funktion der Hardware und das Erstellen von Modelines detailliert beschrieben wird. Eine deutsche Einführung in dieses Thema findet sich im XFree-Kapitel in [21].

Glücklicherweise ist mittlerweile die manuelle Erstellung von Modelines oder Monitordefinitionen fast nie mehr nötig. Wenn Sie einen modernen Multisync-Monitor verwenden, können die zulässigen Frequenzbereiche und optimalen Auflösungen in der Regel, wie im SaX2 Konfigurationsabschnitt erwähnt, direkt via DDC vom X-Server aus dem Monitor gelesen werden. Sollte dies nicht möglich sein, können Sie auch einen der eingebauten VESA-Modi des X-Servers verwenden. Diese sollten auf praktisch allen Grafikkarten/Monitorkombinationen einwandfrei funktionieren.

12.2 Installation und Konfiguration von Fonts

Das Installieren zusätzlicher Fonts unter SUSE LINUX ist sehr einfach. Es genügt die Fonts in ein beliebiges Verzeichnis zu kopieren, das sich im X11 Font-Pfad (siehe Abschnitt 12.2.1 auf Seite 316) befindet und, damit die Fonts auch über das neue Xft-Fontrendering-System benutzbar sind, auch ein Unterverzeichnis der in `/etc/fonts/fonts.conf` konfigurierten Verzeichnisse ist (siehe Abschnitt 12.2.1 auf der nächsten Seite).

Sie können die Fontdateien manuell als `root` in solch ein geeignetes Verzeichnis kopieren, zum Beispiel nach `/usr/X11R6/lib/X11/fonts/truetype/`, oder auch den KDE Fontinstaller im KDE Kontrollzentrum dazu benutzen. Das Ergebnis ist identisch.

Anstelle die Fonts tatsächlich zu kopieren, können Sie natürlich auch symbolische Links anlegen, wenn Sie zum Beispiel lizensierte Fonts auf einer gemounteten Windows Partition haben und diese nutzen möchten. Anschließend rufen Sie `SuSEconfig --module fonts` auf.

`SuSEconfig --module fonts` ruft das Skript `/usr/sbin/fonts-config` auf, das die Konfiguration der Fonts übernimmt. Für Details was dieses Skript tut, lesen Sie bitte die zugehörige Manual-Page (`man fonts-config`).

Es spielt keine Rolle, welche Typen von Fonts installiert werden sollen, die Prozedur ist die gleiche für Bitmap-Fonts, TrueType/OpenType-Fonts und Type1-(PostScript)-Fonts. Alle diese Fontarten können in jedes beliebige Verzeichnis installiert werden. Lediglich CID-keyed Fonts sind ein Spezialfall, siehe Abschnitt 12.2.1 auf Seite 318.

12.2.1 Details zu Font-Systemen

XFree enthält zwei völlig verschiedene Font-Systeme, das alte *X11 Core-Font-System* und das völlig neu entworfene *Xft/fontconfig* System. Im Folgenden wird auf beide Systeme kurz eingegangen.

Xft

Beim Entwurf von Xft wurde von Anfang an darauf geachtet, dass es skalierbare Fonts, inclusive Antialiasing, gut unterstützt. Bei Benutzung von Xft werden die Fonts im Gegensatz zum X11 Core-Font-System von dem Programm gerendert, welches die Fonts benutzt und nicht vom X-Server. Dadurch bekommmt das jeweilige Programm Zugriff auf die Fontdateien selbst und volle Kontrolle über Details, wie die Glyphen genau gerendert werden. Zum einen wird dadurch die korrekte Darstellung von Text in manchen Sprachen erst möglich, zum anderen ist der direkte Zugriff auf die Fontdateien sehr hilfreich, um Fonts zum Drucken zu einzubetten (engl. *to embed*) und so zu erreichen, dass der Ausdruck tatsächlich so aussieht wie die Bildschirmausgabe.

Die beiden Desktopumgebungen KDE und Gnome, Mozilla und viele andere Applikationen benutzen unter SUSE LINUX bereits standardmäßig Xft. Xft wird also bereits von erheblich mehr Applikationen benutzt als das alte X11 Core-Font-System.

Xft benutzt die Fontconfig-Bibliothek um Fonts zu finden und um die Art und Weise wie sie gerendert werden zu beeinflussen. Das Verhalten von fontconfig wird durch eine systemweite Konfigurationsdatei `/etc/fonts/fonts.conf` und eine benutzerspezifische Konfigurationsdatei `~/.fonts.conf` gesteuert. Jede dieser fontconfig Konfigurationsdateien muss mit

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

beginnen und mit

```
</fontconfig>
```

enden. Um Verzeichnisse, in denen nach Fonts gesucht wird hinzuzufügen, können Sie Zeilen wie die folgende

```
<dir>/usr/local/share/fonts/</dir>
```

hinzufügen. Das ist aber selten nötig. Das benutzerspezifische Verzeichnis `~/.fonts/` ist bereits per Default in `/etc/fonts/fonts.conf` eingetragen. Wenn ein Benutzer also für sich persönlich zusätzliche Fonts installieren möchte, genügt es, diese nach `~/.fonts` zu kopieren.

Sie können auch Regeln einfügen, um das Aussehen der Fonts zu beinflussen, zum Beispiel

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

um das Antialiasing für alle Fonts auszuschalten, oder

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

wenn Sie es nur für bestimmte Fonts ausschalten möchten.

Die meisten Applikationen benutzen standardmäßig die Fontnamen `sans-serif` (oder das äquivalente `sans`), `serif` oder `monospace`. Dies sind keine wirklich existierenden Fonts sondern nur Aliases, die abhängig von der eingestellten Sprache auf einen geeigneten Font aufgelöst werden.

Jeder Benutzer kann sich leicht Regeln zu seiner `~/.fonts.conf` hinzufügen um zu erreichen, dass diese Aliases auf seine Lieblingsfonts aufgelöst werden:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
```

```
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Weil fast alle Applikationen diese Aliase standardmäßig verwenden, wirkt das fast für das ganze System. Sie bekommen so mit sehr geringem Aufwand Ihre Lieblingsfonts fast überall, ohne in jedem Program einzeln die Fonteinstellungen ändern zu müssen.

Um festzustellen, welche Fonts überhaupt installiert und verfügbar sind, gibt es das Kommando `fc-list`.

`fc-list ""` gibt zum Beispiel eine Liste aller Fonts aus. Möchten Sie wissen, welche skalierbaren Fonts (`:outline=true`) verfügbar sind, die alle für Hebräisch benötigen Glyphen enthalten (`:lang=he`), und sich für alle diese Fonts den Fontnamen (`family`), den Stil (`style`), den Fettheitsgrad (`weight`) und den Dateinamen, der den Font enthält ausgeben lassen, können Sie zum Beispiel folgendes Kommando benutzen:

```
fc-list ":lang=he:outline=true" family style weight file
```

Die Ausgabe dieses Kommandos könnte zum Beispiel so aussehen:

```
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBold.ttf: FreeSans:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSerif.ttf: FreeSerif:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMono.ttf: FreeMono:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSans.ttf: FreeSans:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Die wichtigsten Parameter, die mit `fc-list` abgefragt und ausgegeben werden können, sind:

Tabelle 12.2: *Mögliche Parameter von fc-list*

Parameter	Bedeutung und mögliche Werte
family	Der Name der Fontfamilie, zum Beispiel `FreeSans`
foundry	Der Fonthersteller, zum Beispiel `urw`
style	Der Fontstil, zum Beispiel `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`, ...
lang	Die Sprache(n), die der Font unterstützt. Zum Beispiel `de` für Deutsch, `ja` für Japanisch, `zh-TW` für traditionelles Chinesisch, `zh-CN` für vereinfachtes Chinesisch ...
weight	Der *Fettheitsgrad*, zum Beispiel `80` für nicht fett, `200` für fett.
slant	Der *Kursivitätsgrad*, meist `0` für nicht kursiv, `100` für kursiv.
file	Der Dateiname unter dem der Font gespeichert ist.
outline	`true` wenn es sich um einen Outline-Font handelt, sonst `false`.
scalable	`true` wenn es sich um einen skalierbaren Font handelt, sonst `false`.
bitmap	`true` wenn es sich um einen Bitmap-Font handelt, sonst `false`.
pixelsize	Die Größe des Fonts in Pixel. Im Zusammenhang mit fc-list nur sinnvoll für Bitmap-Fonts.

X11 Core-Fonts

Heutzutage unterstützt auch das X11 Core-Font-System nicht nur Bitmap-Fonts, sondern auch skalierbare Fonts wie Type1-Fonts, TrueType/OpenType-Fonts und auch CID-keyed Fonts. Auch Unicode-Fonts werden bereits seit längerer Zeit unterstützt.

Ursprünglich wurde wurde das X11 Core-Font-System 1987 für X11R1 entwickelt um monochrome Bitmap-Fonts zu verarbeiten und man merkt bis heute, dass alle oben erwähnten Erweiterungen nachträglich hinzugefügt wurden.

Zum Beispiel werden skalierbare Fonts nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden großer, skalierbarer Fonts mit Glyphen für viele Sprachen kann sehr langsam sein. Auch die Benutzung von Unicode Fonts kann langsam sein und benötigt mehr Speicher.

Es gibt einige grundlegende Schwächen des X11 Core-Font-Systems. Man kann sagen, dass es veraltet und nicht mehr sinnvoll erweiterbar ist. Es muss aus Gründen der Rückwärtskompatibilität verfügbar bleiben, aber soweit wie möglich sollte man das modernere Xft/fontconfig System verwenden.

Beachten Sie bitte, dass nur Verzeichnisse vom X-Server beachtet werden, die

- im Abschnitt `Files` der Datei `/etc/X11/XF86Config` als `FontPath` eingetragen sind.
- eine gültige `font.dir` Datei besitzen (wird von SuSEconfig generiert).
- nicht zur Laufzeit des X-Servers mit Hilfe des Kommandos `xset -fp` abgemeldet wurden.
- bzw. zur Laufzeit des X-Servers mit Hilfe des Kommandes `xset +fp` eingebunden wurden.

Wenn der X-Server bereits läuft, können neu installierte Fonts in bereits eingebundenen Verzeichnisse mit dem Kommando `xset fp rehash` zur Verfügung gestellt werden. Dieses Kommando wird von `SuSEconfig --module fonts` bereits aufgerufen.

Da das Kommando `xset` Zugriff auf den laufenden X-Server benötigt, kann das allerdings nur funktionieren, wenn `SuSEconfig --module fonts` aus einer Shell gestartet wurde, die Zugriff auf den laufenden X-Server hat. Am einfachsten ereichen Sie dies, indem Sie sich durch Eingeben des Kommandos `sux` und anschließende Eingabe des Root-Passwortes in einem Terminal zu `root` machen, `sux` übergibt die Zugriffsrechte des Benutzers, der den X-Server gestartet hat, an die Rootshell.

Zum Testen, ob die Fonts richtig installiert wurden und tatsächlich über das X11 Core-Font-System verfügbar sind, können Sie das Kommando `xlsfonts` verwenden, das alle verfügbaren Fonts auflistet.

SUSE LINUX verwendet standardmäßig UTF-8 Locales, daher sollten Sie in der Regel Unicode-Fonts verwenden, die Sie daran erkennen, dass der von `xlsfonts` gelistete Fontname mit `iso10646-1` endet. Alle verfügbaren Unicode-Fonts können Sie sich also mit `xlsfonts | grep iso10646-1` anzeigen lassen.

Fast alle unter SUSE LINUX verfügbaren Unicode-Fonts enthalten mindestens alle nötigen Glyphen für die europäischen Sprachen, für die früher die Encodings `iso-8859-*` verwendet wurden.

CID-keyed Fonts

Im Gegensatz zu den anderen Fonttypen ist es bei CID-keyed Fonts nicht egal, in welches Verzeichnis sie installiert werden. Sie sollten auf jeden Fall nach `/usr/share/ghostscript/Resource/CIDFont/` installiert werden. Für Xft/fontconfig spielt das zwar keine Rolle, aber Ghostscript und das X11 Core-Font-System erfordern dies.

Hinweis

Weitere Informationen zum Thema Fonts unter X11 erhalten Sie unter `http://www.xfree86.org/current/fonts.html`.

Hinweis

12.3 Konfiguration von OpenGL/3D

Direct3D ist unter Linux nur auf x86- und kompatiblen Systemen als Teil des Windows-Emulators WINE verfügbar, der wiederum das OpenGL-Interface zur Implementierung verwendet.

12.3.1 Hardwareunterstützung

SUSE LINUX beinhaltet für die 3D-Hardwareunterstützung diverse OpenGL-Treiber. Eine Übersicht finden Sie in der Tabelle 12.3.

Tabelle 12.3: *Unterstützte 3D-Hardware*

OpenGL Treiber	Unterstützte Hardware
nVidia	nVidia Chips: alle außer Riva 128(ZX)
DRI	3Dfx Voodoo Banshee, 3Dfx Voodoo-3/4/5, Intel i810/i815/i830M, Intel 845G/852GM/855GM/865G, Matrox G200/G400/G450/G550, ATI Rage 128(Pro)/Radeon

Bei einer Neuinstallation mit YaST kann bereits während der Installation die 3D-Unterstützung aktiviert werden, wenn eine entsprechende Unter-

stützung von YaST erkannt wird. Bei Grafikchips von nVidia muss vorher noch der nvidia-Treiber eingespielt werden. Wählen Sie dazu bitte während der Installation den nVidia-Treiber Patch in YOU (YaST Online Update) an. Aus Lizenzgründen können wir den nVidia-Treiber leider nicht mitliefern.

Sollte ein Update eingespielt worden sein, muss der 3D-Hardwaresupport anderweitig eingerichtet werden. Die Vorgehensweise hängt dabei vom zu verwendenden OpenGL-Treiber ab und wird im folgenden Abschnitt genauer erklärt.

12.3.2 OpenGL-Treiber

nVidia und DRI

Diese OpenGL-Treiber können sehr komfortabel mit SaX2 eingerichtet werden. Beachten Sie bitte, dass bei nVidia-Karten vorher noch der nVidia-Treiber eingespielt werden muss (s.o.). Mit dem Kommando `3Ddiag` können Sie überprüfen, ob die Konfiguration für nVidia bzw. DRI korrekt ist.

Aus Sicherheitsgründen dürfen nur die Benutzer der Gruppe `video` auf die 3D-Hardware zugreifen. Stellen Sie deshalb sicher, dass alle Benutzer, die auf der Maschine lokal arbeiten, in der Gruppe `video` eingetragen sind. Ansonsten wird für OpenGL-Programme der langsamere *Software Rendering Fallback* des OpenGL-Treibers verwendet. Mit dem Kommando `id` können Sie überprüfen, ob der aktuelle Benutzer der Gruppe `video` angehört. Ist dies nicht der Fall, kann er mittels YaST zu dieser Gruppe hinzugefügt werden.

12.3.3 Diagnose-Tool 3Ddiag

Um die 3D-Konfiguration unter SUSE LINUX überprüfen zu können, steht das Diagnosetool 3Ddiag zur Verfügung. Beachten Sie bitte, dass es sich dabei um ein Kommandozeilentool handelt, das Sie in einem Terminal aufrufen müssen.

Das Programm überprüft beispielsweise die XFree-Konfiguration, ob die entsprechenden Pakete für 3D-Support installiert sind und ob die korrekte OpenGL-Bibliothek sowie GLX Extension verwendet wird. Befolgen Sie bitte die Anweisungen von 3Ddiag, wenn es zu "failed" Meldungen kommt. Im Erfolgsfall werden ausschließlich "done" Meldungen auf dem Bildschirm ausgegeben.

Mit `3Ddiag -h` lassen sich zulässige Optionen für 3Ddiag ermitteln.

12.3.4 OpenGL-Testprogramme

Als OpenGL-Testprogramme eignen sich neben `glxgears` Spiele wie `tuxracer` und `armagetron` (gleichnamige Pakete). Bei aktiviertem 3D-Support sollten sich diese auf einem halbwegs aktuellen Rechner flüssig spielen lassen. Ohne 3D-Support ist dies nicht sinnvoll (Diashow-Effekt). Eine zuverlässige Aussage darüber, ob 3D aktiviert ist, liefert die Ausgabe von `glxinfo`. `direct rendering` muss hier auf `Yes` stehen.

12.3.5 Troubleshooting

Sollte sich der OpenGL 3D-Test ein negatives Ergebnis liefern (kein flüssiges Spielen möglich), sollte erst mit 3Ddiag überprüft werden, ob keine Fehlkonfiguration vorliegt (`failed` Meldungen) und diese ggf. behoben werden. Hilft auch das nicht oder lagen keine failed Meldungen vor, hilft oft nur noch ein Blick in die Logdateien von XFree86. Oft findet man hier in `/var/log/XFree86.0.log` von XFree86 die Zeile `DRI is disabled`. Dafür kann es mehrere Ursachen geben, die sich jedoch nur mit genauem Studium der Logdatei finden lassen, womit der Laie in aller Regel überfordert ist.

In diesen Fällen liegt in der Regel kein Konfigurationsfehler vor, da dieser bereits von 3Ddiag erkannt worden wäre. Somit bleibt ohnehin nur der Software Rendering Fallback des DRI Treibers, der jedoch keinerlei 3D-Hardware-Support bietet. Man sollte ebenfalls auf die Verwendung von 3D-Support verzichten, wenn sich OpenGL Darstellungsfehler oder gar Stabilitätsprobleme ergeben. Verwenden Sie SaX2 um den 3D-Support zu deaktivieren.

12.3.6 Installationssupport

Abgesehen von Software Rendering Fallback des DRI Treibers befinden sich unter Linux alle OpenGL-Treiber im Entwicklungsstadium und sind deshalb zum Teil noch als experimentell anzusehen. Wir haben uns dennoch entschlossen, die Treiber auf der Distribution mitzuliefern, da die Nachfrage nach 3D-Hardwarebeschleunigung unter Linux sehr groß ist. Aufgrund des z.T. experimentellen Stadiums der OpenGL-Treiber können wir im Rahmen des Installationssupports jedoch nicht auf das Einrichten von 3D-Hardwarebeschleunigung eingehen und bei diesbezüglichen Problemen nicht weiterhelfen. Das grundlegende Einrichten der grafischen Benutzeroberfläche X11 beinhaltet also keinesfalls auch das Einrichten

von 3D-Hardwarebeschleunigung. Wir hoffen jedoch, dass dieses Kapitel viele Fragen zu diesem Thema beantwortet. Bei Problemen mit dem 3D-Hardwaresupport empfehlen wir Ihnen, im Zweifelsfall auf 3D-Support zu verzichten.

12.3.7 Weiterführende Online-Dokumentation

- DRI: `/usr/X11R6/lib/X11/doc/README.DRI` (`XFree86-doc`)

Druckerbetrieb

In diesem Kapitel werden zunächst Hinweise zum Update von SUSE LINUX Enterprise Server 8 auf SUSE LINUX Enterprise Server 9 gegeben. Dann wird Standardwissen zum Druckerbetrieb geliefert. Es dient insbesondere auch dazu, geeignete Problemlösungen für den Druckerbetrieb in Netzwerken zu finden.

13.1 Update, Upgrade und Migration 324
13.2 Vorbereitungen und weitere Überlegungen 327
13.3 Druckeranbindung — Methoden und Protokolle . 329
13.4 Installation der Software 330
13.5 Konfiguration des Druckers 331
13.6 Besonderheiten bei SUSE LINUX 334
13.7 Mögliche Probleme und deren Lösung 339

13.1 Update, Upgrade und Migration

Mit der Vorgängerversion SuSE Linux Enterprise Server 8 wurden die beiden Drucksysteme LPRng/lpdfilter und CUPS als gleichberechtigte Alternativen ausgeliefert. Mit SUSE LINUX Enterprise Server 9 beginnt der Fokus sich zu CUPS zu verschieben. Die Möglichkeit zur Migration einer mit YaST erstellten LPRng/lpdfilter-Konfiguration in eine CUPS-Konfiguration muss bei SUSE LINUX Enterprise Server 9 entfallen. Daher muss vor einem Update von SuSE Linux Enterprise Server 8 auf SUSE LINUX Enterprise Server 9 entschieden werden, ob noch unter SuSE Linux Enterprise Server 8 eine Migration von LPRng/lpdfilter auf CUPS durchzuführen ist.

CUPS ist das Drucksystem der Zukunft. Auch wenn die Pakete `lprng` und `lpdfilter` weiterhin ausgeliefert werden, empfiehlt sich bei SUSE LINUX Enterprise Server 9 der Umstieg auf CUPS, da es die folgenden Vorteile bietet:

- individuelle Einstellung der Druckparameter auf Benutzer-Ebene
- optimale Unterstützung von PostScript-Druckern
- „Browsing“ im Netzwerk
- Web-Frontend (auf Benutzer-Ebene und zur Administration)

Nach SUSE LINUX Enterprise Server 9 wird die Konfiguration von LPRng/lpdfilter nicht mehr von YaST unterstützt werden, sondern muss ab dann manuell erfolgen. Daher sollte unter SUSE LINUX Enterprise Server 9 zumindest geprüft werden, ob CUPS den Anforderungen genügt und ein Wechsel möglich ist.

13.1.1 Aktualisierung von CUPS

Bei der Aktualisierung von CUPS sind die folgenden beiden Fälle zu unterscheiden:

Update von CUPS Die Softwarepakete werden aktualisiert, aber die bestehenden Konfigurationsdateien werden unverändert übernommen. Nach dem Update werden sich die Warteschlangen und der cupsd wie vorher verhalten; dies bedeutet gleichzeitig, dass viele Neuerungen in SUSE LINUX Enterprise Server 9 zunächst ungenutzt bleiben und bei Bedarf nachträglich hinzukonfiguriert werden müssen.

Upgrade von CUPS Die bestehenden Softwarepakete und die bestehenden Konfigurationsdateien werden durch die neuen Softwarepakete und deren Default-Konfigurationsdateien ersetzt. Alle Neuerungen stehen sofort zur Verfügung, die Warteschlangen müssen jedoch neu angelegt werden. Die Neuerungen sind im einzelnen in den folgenden Artikeln beschrieben:

- `http://portal.suse.com/sdb/de/2004/03/jsmeix_print-einrichten-91.html`
- `http://portal.suse.com/sdb/de/2003/09/jsmeix_print-einrichten-90.html`
- `http://portal.suse.com/sdb/de/2003/03/jsmeix_print-einrichten-82.html`
- `http://portal.suse.com/sdb/de/2002/09/jsmeix_print-einrichten-81.html`

13.1.2 Migration von LPRng/lpdfilter nach CUPS

CUPS und LPRng/lpdfilter sind grundlegend verschieden.

- Bei CUPS sind die Konfigurationsdaten für die Warteschlangen in `/etc/cups/printers.conf` und `/etc/cups/ppd/` gespeichert und `/etc/printcap` wird vom `cupsd` nur zwecks Kompatibilität zu `printcap`-basierten Anwendungsprogrammen angelegt.
- CUPS verwendet das IPP Protokoll, LPRng das LPD Protokoll
- CUPS braucht normalerweise mehr Rechenleistung für die leistungsfähigere Filterung und das Web-Interface

Hinweis

LPD-Funktionalität bei CUPS

CUPS unterstützt grundlegende LPD Funktionalität, und zwar *empfängerseitig* durch den `cups-lpd` und *senderseitig* durch das `lpd`-Backend. CUPS unterstützt jedoch nicht die volle LPRng Funktionalität. Weiterhin ist es möglich, Filterskripte von LPD-basierten Drucksystemen als „System V style interface script“ zu verwenden.

Hinweis

Einsatz eines Testsystems

Durch den Parallelbetrieb eines Testsystems kann man auf eine gesicherte Weise nach CUPS migrieren; dabei bleibt der vorhandene LPD-Druckserver weiterhin aktiv. Auf einem zusätzlichen Testsystem wird SUSE LINUX Enterprise Server 9 mit CUPS installiert.

Das folgende Vorgehen funktioniert nur für Netzwerkdrucker gut; denn wenn Drucker direkt am LPD-Druckserver angeschlossen sind, müssen diese zu Tetszwecken direkt am CUPS-Testsystem angeschlossen werden. Auf dem CUPS-Testsystem werden für die Netzwerkdrucker die Warteschlangen eingerichtet. Dabei ist zu beachten, dass viele Netzwerkdrucker (bzw. deren Netzwerkschnittstellen) überfordert sind, wenn sie von mehreren Rechnern gleichzeitig Daten erhalten. Daher ist während Tests mit dem CUPS-Testsystem das Ausdrucken für die zu testenden Netzwerkdrucker auf dem LPD-Druckserver anzuhalten.

Wenn die Warteschlangen auf dem CUPS-Testsystem mit YaST oder dem Web-Frontend von CUPS oder einem anderen graphischen Tool angelegt werden, sind die vorgenommenen Einstellungen genau zu protokollieren, um diese später genau so auf dem Produktivsystem einrichten zu können. Wenn die Warteschlangen auf dem CUPS-Testsystem aber nur mit `lpadmin`-Kommandos angelegt werden, genügt es, die `lpadmin`-Kommandos in einem Skript festzuhalten und dieses Skript auf dem Produktivsystem laufen zu lassen.

Umstellung des Produktivsystem

Für Warteschlangen, die nur mit YaST konfiguriert wurden:

1. Migration von LPRng/lpdfilter nach CUPS unter SuSE Linux Enterprise Server 8.
2. Update von SuSE Linux Enterprise Server 8 auf SUSE LINUX Enterprise Server 9.

Für Warteschlangen, nicht nur mit YaST konfiguriert wurden, gibt es keinen Automatismus zur Migration. Ein Wechseln der installierten Pakete von LPRng/lpdfilter zu CUPS ist verfügbar, aber eine bestehende Konfiguration wird dabei nicht migriert.

Bei SuSE Linux Enterprise Server 8 werden mit der Druckerkonfiguration von YaST immer die beiden Drucksysteme CUPS und LPRng/lpdfilter gleichzeitig konfiguriert. Die Druckerkonfiguration speichert dazu sämtliche Konfigurationsdaten und legt damit die Konfiguration für das aktuelle

Drucksystem an - bzw. für das neue Drucksystem, wenn das Drucksystem gewechselt wurde. Die YaST-Druckerkonfiguration unterscheidet streng zwischen Warteschlangen, die sie selbst angelegt hat, und solchen, die auf andere Art angelegt wurden. Letztere werden nicht verändert und können auch nicht verändert werden, sondern nur mit einer neuen Konfiguration überschrieben werden.

Bei SUSE LINUX Enterprise Server 9 sind YaST und andere Konfigurationstools (z. B. das CUPS Web-Frontend) synchronisiert. Es gibt keine „privaten“ YaST-Konfigurationsdaten mehr. Die Migration einer mit YaST erstellten LPRng/lpdfilter-Konfiguration in eine CUPS-Konfiguration muss daher bei SUSE LINUX Enterprise Server 9 entfallen, denn zur Migration einer YaST-Konfiguration werden „private“ YaST-Konfigurationsdaten benötigt. Eine automatische Migration einer beliebigen LPRng/lpdfilter-Konfiguration in eine CUPS-Konfigurationen ist nicht mit vertretbarem Aufwand realisierbar.

13.2 Vorbereitungen und weitere Überlegungen

CUPS ist das Standarddrucksystem unter SUSE LINUX. CUPS ist sehr anwederorientiert. In vielen Fällen ist es kompatibel zu LPRng oder kann mit relativ wenig Aufwand dazu gebracht werden. LPRng wird nur noch aus Kompatibilitätsgründen bei SUSE LINUX Enterprise Server mitgeliefert; vgl. den Abschnitt 13.1 auf Seite 324 .

Drucker können hinsichtlich der Schnittstellen (USB, Netzwerk) sowie der Druckersprachen unterschieden werden. Beim Kauf eines Druckers sollte daher sowohl auf eine geeignete Schnittstelle, die von der Hardware unterstützt wird, als auch auf die Druckersprache Wert gelegt werden.

Man kann Drucker grob in etwa die folgenden drei Klassen von Druckersprachen einteilen:

PostScript-Drucker PostScript ist die Druckersprache in der die meisten Druckaufträge unter Linux/Unix erstellt werden und vom Drucksystem intern verarbeitet werden. Die Sprache ist schon sehr alt und sehr mächtig. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet werden können und nicht mehr durch weitere Schritte im Drucksystem umgewandelt werden müssen, so reduziert sich die Anzahl der potentiellen Fehlerquellen. Da PostScript-Drucker lizenziert

werden müssen und dabei anfallende Kosten nicht unerheblich sind, kosten diese Drucker im allgemeinen mehr als Drucker, die mit keinem PostScript-Interpreter ausgerüstet sind.

Standarddruckersprachen wie PCL und ESC/P
Diese Druckersprachen sind sehr alt, werden aber auch heute noch erweitert, um aktuelle Entwicklungen im Drucker ansteuern zu können. Wenn es sich um bekannte Druckersprachen handelt, kann das Drucksystem PostScript-Aufträge mit Hilfe von Ghostscript in die Druckersprache umwandeln („interpretieren“ genannt). Die bekanntesten sind PCL, welches hauptsächlich bei HP-Druckern und deren „Clones“, und ESC/P, welches bei Epson-Druckern verbreitet ist. Bei solchen Druckersprachen kann man meist davon ausgehen, dass sie unter auch Linux zu guten Druckergebnissen führen. Mit Ausnahme der `hpijs`-Treiber, die von HP selbst entwickelt werden, gibt es derzeit (2004) keinen Druckerhersteller, der Linux-Treiber entwickelt und diese unter einer OpenSource-Lizenz den Linux-Distributoren zur Verfügung stellt.

Vom Preissegment her bewegen sich diese Drucker meist im mittleren Bereich.

Proprietäre Drucker, meist GDI-Drucker
Für die Klasse der proprietären Drucker gibt es meist nur einen oder mehrere Windows-Treiber. Bei diesen Druckern ist keine der bekannten Druckersprache implementiert und die Druckersprache als solche kann sich von einem Modelljahrgang zum nächsten ändern.

Die OpenSource-Gemeinde hat es mittlerweile aufgegeben, solche Drucker per Reverse-Engineering zu unterstützen, da sich nach einem langen Aufwand nur ein sehr kurzer Moment des Erfolgs einstellt. Günstige Lexmark-Drucker sind hier typische Vertreter, die mittlerweile auch unter dem Produktnamen Dell angeboten werden. Diese Drucker finden sich meist als „Dreingabe“ in einem PC-Bundle und man erkennt sie daran, dass ein Set Nachfüllpatronen meist teurer ist als der Kaufpreis des Druckers.

Diese Drucker finden sich meist im billigsten Preissegment. Unter Linux sind sie meistens nicht verwendbar.

Vor einer Neuanschaffung sollte man die folgenden Informationsquellen konsultieren, um Unterstützungsgrad des in Aussicht genommenen Druckers in Erfahrung zu bringen:

- `http://cdb.suse.de/` bzw. `http://hardwaredb.suse.de/` — die SUSE LINUX Druckerdatenbank

- `http://www.linuxprinting.org/` — die Druckerdatenbank auf Linuxprinting.org
- `http://www.cs.wisc.edu/~ghost/` — die Ghostscript-Webseite
- `file:/usr/share/doc/packages/ghostscript/catalog.devices` — die eingebundenen Treiber

Natürlich geben die Online-Datenbanken immer den aktuellsten Stand der Linux-Unterstützung an und ein Produkt kann nur bis zum Produktionszeitpunkt aktuelle Treiber einbinden; ein aktuell als „perfekt unterstützter“ eingestufter Drucker muss dies zum Zeitpunkt der Produktion von SUSE LINUX noch nicht gewesen sein. Die Datenbanken geben also nicht notwendigerweise immer den korrekten Zustand an, sondern nur in guter Näherung.

13.3 Druckeranbindung — Methoden und Protokolle

Es gibt verschiedene Möglichkeiten, um einen Drucker an das System anzuschließen. Für das CUPS-Drucksystem ist es von der Konfiguration her unerheblich, ob ein Drucker lokal oder über das Netzwerk mit dem System verbunden ist.

Lokale Drucker sind unter Linux genauso anzuschließen, wie es der Druckerhersteller in der Anleitung vorschreibt. Von CUPS werden die folgende Anschlussarten unterstützt: seriell, USB, parallel und SCSI. Das entsprechende Backend muss auch zur Kommunikation gewählt werden.

► **S/390, zSeries**
Die an S/390- und zSeries-Mainframes lokal anschließbaren Drucker sowie die entsprechenden virtuellen Geräte, die von z/VM zur Verfügung gestellt werden, werden von CUPS und lprng nicht unterstützt. Auf diesen Plattformen ist nur das Drucken per Netzwerk möglich. ◄

Achtung

Kabelverbindung zum Rechner

Beim Verkabeln mit dem Rechner muss man darauf achtgeben, dass nur USB-Verbindungen darauf ausgelegt sind, im laufenden Betrieb angeschlossen oder getrennt zu werden. Alle anderen Verbindungen sollte man immer nur im ausgeschalteten Betrieb ändern.

Achtung

Bei Netzwerkdruckern geschieht die Verkabelung ebenso wie vom Druckerhersteller beschrieben.

13.4 Installation der Software

„PostScript Printer Description“ (PPD) ist die Computersprache, die Eigenschaften (z. B. Auflösung) und Optionsmöglichkeiten (z. B. Duplex-Einheit) von Druckern beschreibt; vgl. Abschnitt 13.6.3 auf Seite 336. Diese Beschreibungen sind notwendig, um die verschiedenen Optionen des Druckers unter CUPS nutzen zu können. Ohne PPD-Datei werden die Druckdaten „roh“ an den Drucker weitergegeben, was man im allgemeinen nicht wünscht.

Mit SUSE LINUX sind schon viele PPD-Dateien vorinstalliert, um gerade auch Drucker, die PostScript von hause aus nicht unterstützen, verwenden zu können.

Falls ein PostScript-Drucker konfiguriert ist, empfiehlt es sich die passende PPD-Datei zu besorgen. Falls sich dies als zu viel Aufwand erweist oder eine solche nicht besorgt werden kann oder möglicherweise gar nicht existiert, kann auch eine generische PPD-Datei, die mit dem System mitgeliefert wird, benutzt werden. Üblicherweise findet man sonst PPD-Dateien auf den Treiber-CDs für Windows oder Apple MacOS, die bei syntaktischer Korrektheit ohne Probleme auch unter Linux verwendet werden können. Die Druckerhersteller bieten manchmal auch im Internet PPD-Dateien an.

Neue PPD-Dateien sind im Verzeichnis `/usr/share/cups/model/` abzulegen oder besser per YaST in das Drucksystem hinzufügen; vgl. den Abschnitt 2.4.3 auf Seite 76 . Dann wird eine solche PPD-Datei bevorzugt bei der Installation gewählt.

Mit Vorsicht ist dagegen zu genießen, wenn ein Druckerhersteller neben Konfigurationsdaten verlangt, dass ganze Software-Pakete installiert werden sollen. Durch eine solche Installation würde man zum einen den Support von Seiten SUSE LINUX verlieren, und zum anderen darf man sich dann nicht wundern, wenn Druck-Kommandos anders als bisher funktionieren und Geräte anderer Hersteller gar nicht angesprochen werden können. Von daher ist i. a. von einer Installation von Hersteller-Software abzuraten.

13.5 Konfiguration des Druckers

Nachdem der Drucker mit dem Computer verbunden und die Software installiert ist, gilt es, diesen im System zu konfigurieren. Dabei sollten die mit SUSE LINUX gelieferten Tools verwendet werden und möglichst keine anderen. Da bei SUSE LINUX hoher Wert auf Sicherheit gelegt wird, kommen 3rd-Party-Tools mit den Sicherheitseinschränkungen nicht immer klar und führen am Ende zu mehr Komplikationen als dass sie helfen.

13.5.1 Lokaler Drucker

Wurde ein lokaler Drucker beim Einloggen als noch nicht konfiguriert erkannt, so wird ein YaST-Modul zur Konfiguration wird gestartet; vgl. den Abschnitt 2.4.3 auf Seite 75 .

Zum Konfigurieren mit Kommandozeilen-Tools (s. u.) ist eine eine Device-URI notwendig. Diese lautet beispielsweise: `parallel:/dev/lp0` (Drucker am 1. Parallel-Port) `usb:/dev/usb/lp1` (1. erkannter Drucker am USB-Port).

13.5.2 Netzwerkdrucker

Ein Netzwerkdrucker kann verschiedene Protokolle unterstützen und manche davon sogar gleichzeitig. Die meisten der unterstützten Protokolle sind standardisiert und trotzdem kann es vorkommen, dass Hersteller den Standard erweitern (abändern), weil sie entweder mit Systemen testen, die den Standard nicht korrekt implementiert haben, oder weil sie bestimmte Funktionen haben möchten, die es laut Standard gar nicht gibt. Derartige Treiber bieten sie nur für einige wenige Betriebssysteme an, zu denen Linux leider nur in seltenen Fällen gehört.

Es kann also im Moment also nicht davon ausgegangen werden, dass jedes Protokoll unter Linux problemlos funktioniert und daher sollte durchaus mit den verschiedenen Möglichkeiten experimentiert werden, um zu einer funktionstüchtigen Konfiguration zu gelangen.

Unter CUPS werden die Protokolle `socket`, `LPD`, `IPP` und `smb` unterstützt. Im Folgenden einige Detailinformationen zu diesen Protokollen:

socket „socket“ bezeichnet die Verbindung, bei der die Daten auf einen Internetsocket geschickt werden, ohne dass vorher ein Daten-Handshake ausgeführt wird. Typisch verwendete Socket-Port-Nummern sind `9100` oder `35`. Beispiel für eine Device-URI: `socket://`⟨*host-printer*⟩`:9100/`

LPD (Line Printer Daemon) Das LPD-Protokoll ist traditionell bewährt. LPD steht für "Line Printer Daemon" und es wird im RFC 1179 beschrieben. Dieses Protokoll beinhaltet, dass vor den eigentlich Druckdaten noch ein paar wenige auftragsbezogene Daten verschickt werden, z.B. Druckerqueue. Daher ist es notwendig, dass bei der Konfiguration des LPD-Protokolls zur Datenübertragung auch eine Druckerqueue angegeben wird. Implementierungen diverser Druckerhersteller sind so flexibel geschrieben, dass sie jeden Namen als Druckerqueue akzeptieren. Den zu verwendenden Namen findet man im Bedarfsfall im Handbuch zum Drucker. Häufig lauten sie LPT, LPT1, LP1 oder so ähnlich. Natürlich kann man auf diese Weise auch eine LPD-Queue an einem anderen Linux- oder unix-artigen Rechner im CUPS-System konfigurieren. Die Port-Nummer für einen LPD-Dienst lautet `515`. Beispiel für eine Device-URI: `lpd://`⟨*`host-printer`*⟩`/LPT1`

IPP (Internet Printing Protokoll) Das Internet Printing Protokoll, kurz IPP, ist noch relativ jung (1999) und basiert auf dem Protokoll HTTP. Es werden im IPP deutlich mehr auftragsbezogene Daten verschickt als in den anderen Protokollen. CUPS verwendet zur internen Datenübertragung das IPP. Sollte eine Forwarding-Queue zwischen zwei CUPS-Server eingerichtet werden, so ist dieses Protokoll zu bevorzugen. Auch hier wird wieder der Name der Druckerqueue benötigt, um IPP korrekt konfigurieren zu können. Die Port-Nummer für IPP lautet `631`. Beispiel für eine Device-URI: `ipp://`⟨*`host-printer`*⟩`/ps` oder: `ipp://`⟨*`host-cupsserver`*⟩`/printers/ps`

SMB (Windows-Share) Schließlich unterstützt CUPS auch noch das Drucken auf Drucker am Windows-Share. Das Protokoll hierfür lautet SMB und es werden die Port-Nummer `137`, `138` und `139` verwendet. Beispiel für eine Device-URI: `smb://`⟨*`user`*⟩`:`⟨*`password`*⟩`@`⟨*`workgroup`*⟩`/`⟨*`server`*⟩`/`⟨*`printer`*⟩ oder: `smb://`⟨*`user`*⟩`:`⟨*`password`*⟩`@`⟨*`host`*⟩`/`⟨*`printer`*⟩ oder: `smb://`⟨*`server`*⟩`/`⟨*`printer`*⟩

Das vom Drucker unterstützte Protokoll ist also vor der Konfiguration herauszufinden. Sollte sich der Hersteller darüber ausschweigen, so kann es mit Hilfe des Befehls `nmap` (Paket `nmap`) erraten werden. `nmap` prüft einen Host nach offenen Ports; Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000
```

13.5.3 Konfigurationsarbeiten

Netzwerkdrucker konfigurieren

Netzwerkdrucker sind mit YaST einzurichten; YaST erleichtert die Konfiguration und es kann am besten mit den Sicherheitseinschränkungen bei CUPS umgehen; vgl. auch den Abschnitt 13.6.1 auf der nächsten Seite .

Konfiguration per Kommandozeilen-Tools

Alternativ ist es auch möglich, mit Kommandozeilentools CUPS zu konfigurieren. Wenn die Vorarbeit schon gemacht ist (PPD-Datei ist bekannt und der Name der Device-URI auch), sind nur noch die folgenden Schritte notwendig:

```
lpadmin -p <queuename> -v <Device-URI> \
  -P <PPD-Datei> -E
```

Dabei ist wichtig, dass das `-E` nicht die erste Option ist. Denn bei allen CUPS-Befehlen bedeutet `-E` als erstes Argument, dass eine verschlüsselte Verbindung benutzt werden soll (engl. encrypted) und nicht, wie oben beabsichtigt, der Drucker aktiviert werden soll (engl. enable). Konkretes Beispiel:

```
lpadmin -p ps -v parallel:/dev/lp0 \
  -P /usr/share/cups/model/Postscript.ppd.gz -E
```

Analoges Beispiel für einen Netzwerkdrucker:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ \
  -P /usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Optionen verändern

YaST bietet an, dass schon zur Installation bestimmte Optionen als Vorgabe („per default“) aktiviert sind. Diese lassen sich pro Printjob verändern (abhängig von dem verwendeten Printtool), es ist aber auch möglich, diese Einstellungen später noch festzulegen (z. B. mit YaST).

Mit den Kommandozeilen-Tools lässt sich das wie folgt bewerkstelligen:

1. Zuerst lässt man sich alle Optionen ausgeben:

   ```
   lpoptions -p <queue> -l
   ```

Beispiel:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi 1200dpi
```

2. Die aktivierte Default-Option erkennt man am vorgestellten Asterisk: *

3. Eine neue Option dann mit `lpadmin` ändern:

```
lpadmin -p <queue> -o Resolution=600dpi
```

4. Überprüfen, ob nichts schief ging:

```
lpoptions -p <queue> -l

Resolution/Output Resolution: 150dpi 300dpi *600dpi 1200dpi
```

13.6 Besonderheiten bei SUSE LINUX

13.6.1 Web-Frontend (CUPS) und KDE-Administration

Um die Administration mit dem Web-Frontend (CUPS) oder dem Drucker-Administrationstool (KDE) nutzen zu können, muss der Benutzer `root` als CUPS-Administrator mit der CUPS-Administrationsgruppe `sys` und einem CUPS-Passwort angelegt werden; dies erreicht man als `root` mit folgendem Befehl:

```
lppasswd -g sys -a root
```

Andernfalls ist die Administration via Web-Interface oder via Administrationstool nicht möglich, denn die Authentisierung schlägt fehl, wenn kein CUPS-Administrator eingerichtet ist. Anstelle von `root` kann auch ein anderer Benutzer als CUPS-Administrator bestimmt werden; vgl. den folgenden Abschnitt 13.6.2 .

13.6.2 Änderungen beim cupsd

Beim CUPS-Druckdienst gibt es drei wichtige Änderungen:

- Der `cupsd` läuft als Benutzer `lp`.

- Verallgemeinerte Funktionalität für BrowseAllow/BrowseDeny.
- Der cupsd wird standardmäßig aktiviert.

Genauere Informationen dazu finden Sie im Support-Datenbank Artikel „Drucker einrichten ab SUSE LINUX 9.0“ unter `http://portal.suse.com/sdb/de/2003/09/jsmeix_print-einrichten-90.html`.

Der cupsd läuft als Benutzer lp

Der `cupsd` wechselt nach dem Start vom Benutzer `root` zum Benutzer `lp`. Dadurch erhöht sich die Sicherheit, weil der CUPS-Druckdienst nicht mit unbeschränkten Rechten läuft, sondern nur mit solchen Rechten, die für den Druckdienst notwendig sind.

Ein Nachteil ist jedoch, dass die Authentisierung (genauer: die Passwortprüfung) nicht mittels `/etc/shadow` erfolgen kann, denn `lp` hat auf `/etc/shadow` keinen Zugriff. Stattdessen muss die CUPS-spezifische Authentisierung via `/etc/cups/passwd.md5` verwendet werden. Dazu muss ein CUPS-Administrator mit der CUPS-Administrationsgruppe `sys` und einem CUPS-Passwort in `/etc/cups/passwd.md5` eingetragen werden; als als Benutzer `root` ist einzugeben:

```
lppasswd -g sys -a <CUPS-admin-name>
```

Weitere Konsequenzen:

- Wenn der `cupsd` als `lp` läuft, kann `/etc/printcap` nicht erzeugt werden, denn `lp` darf in /etc/ keine Dateien anlegen. Deswegen legt cupsd `/etc/cups/printcap` an. Damit Anwendungsprogramme, die die Warteschlangennamen nur aus `/etc/printcap` lesen können, weiterhin korrekt funktionieren ist `/etc/printcap` ist ein symbolischer Link auf `/etc/cups/printcap`.
- Sobald der cupsd als `lp` läuft, kann der Port 631 nicht geöffnet werden. Deswegen kann der cupsd nicht mehr mit `rccups reload` neu geladen werden. Stattdessen sollte `rccups restart` verwendet werden.

Verallgemeinerte Funktionalität für BrowseAllow/BrowseDeny

Die bei BrowseAllow und BrowseDeny gesetzten Zugfriffsbedingungen beziehen sich auf alle Arten von Paketen, die an den cupsd geschickt werden. Die defaultmäßigen Einstellungen in `/etc/cups/cupsd.conf` sind:

```
BrowseAllow @LOCAL
BrowseDeny All
```

und

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

Damit können genau die `LOCAL`-Rechner auf den cupsd auf einem CUPS-Server zugreifen. `LOCAL`-Rechner sind solche, deren IP-Adresse zu einem nicht-point-to-point Interface gehört (genauer: Interfaces deren `IFF_POINTOPOINT` Flag nicht gesetzt ist) und deren IP-Adresse zum gleichen Netzwerk wie der CUPS-Server gehört. Von allen anderen Rechnern werden jegliche Pakete sofort zurückgewiesen.

Der cupsd wird standardmässig aktiviert

Bei einer Standardinstallation wird der cupsd automatisch aktiviert. Das ermöglicht ohne zusätzliche manuelle Aktionen den komfortablen Zugriff auf Warteschlangen von CUPS-Netzwerk-Servern.

Die beiden obigen Punkte sind dafür notwendige Bedingungen, denn andernfalls wäre die Sicherheit nicht hinreichend für eine automatische Aktivierung des cupsd.

13.6.3 PPD-Dateien in SUSE Linux-Paketen

Druckerkonfiguration nur mit PPD-Dateien

Die YaST-Druckerkonfiguration legt die Warteschlangen für CUPS nur mit den auf dem jeweiligen System unter `/usr/share/cups/model/` installierten PPD-Dateien an. Für ein bestimmtes Druckermodell ermittelt YaST die passenden PPD-Dateien indem der bei der Hardwareerkennung ermittelte Hersteller- und Modellname mit den Hersteller- und Modellnamen in allen auf dem jeweiligen System unter `/usr/share/cups/model/` vorhandenen PPD-Dateien verglichen wird. Die YaST-Druckerkonfiguration baut dazu eine Datenbank aus den Hersteller- und Modell-Informationen, die in den PPD-Dateien stehen, auf. Dadurch können Sie Ihren Drucker

über die Hersteller- und Modellbezeichnung auswählen und erhalten somit die PPD-Dateien, die zu dieser Hersteller- und Modellbezeichnung passen.

Das Konfigurieren nur mit den PPD-Dateien und ohne sonstige Informationsquellen hat den Vorteil, dass die PPD-Dateien unter `/usr/share/cups/model/` beliebig geändert werden können. Die YaST-Druckerkonfiguration erkennt Veränderungen und baut dann die Hersteller/Modell-Datenbank erneut auf. Wenn Sie beispielsweise nur PostScript-Drucker haben, dann brauchen Sie normalerweise weder die Foomatic PPD-Dateien im Paket cups-drivers noch die GimpPrint PPD-Dateien im Paket cups-drivers-stp, sondern Sie können die genau zu Ihren PostScript-Druckern passenden PPD-Dateien nach `/usr/share/cups/model/` kopieren (wenn diese nicht schon im Paket manufacturer-PPDs vorhanden sind) und so Ihre Drucker optimal konfigurieren.

CUPS PPD-Dateien im Paket cups

Die generischen PPD-Dateien im Paket cups wurden speziell für PostScript Level 2 und Level 1 Drucker um folgende angepasste Foomatic PPD-Dateien ergänzt: `/usr/share/cups/model/Postscript-level1.ppd.gz` `/usr/share/cups/model/Postscript-level2.ppd.gz`

Foomatic (bzw. LinuxPrinting.org) PPD-Dateien im Paket cups-drivers

Für Nicht-PostScript-Drucker wird normalerweise der Foomatic Druckerfilter "foomatic-rip" zusammen mit Ghostscript verwendet. Die dazu passenden Foomatic PPD-Dateien sind durch die Einträge "*NickName: ... Foomatic/⟨*Ghostscript Treiber*⟩" und "*cupsFilter: ... foomatic-rip" gekennzeichnet. Diese PPD-Dateien befinden sich im Paket cups-drivers.

YaST verwendet bevorzugt eine Foomatic PPD-Datei, wenn folgende Bedingungen erfüllt sind:

- Es passt eine "recommended" Foomatic PPD-Datei zu dem Druckermodell, die duch den Eintrag "*NickName: ... Foomatic ... (recommended)" gekennzeichnet ist.
- Es gibt keine PPD-Datei aus manufacturer-PPDs, die besser geeignet ist (siehe unten).

GimpPrint PPD-Dateien im Paket cups-drivers-stp

Für viele Nicht-PostScript-Drucker kann statt "foomatic-rip" alternativ auch der CUPS-Filter "rastertoprinter" von GimpPrint verwendet werden. Dieser

Filter und die dazu passenden GimpPrint PPD-Dateien sind im Paket cups-drivers-stp. Die GimpPrint PPD-Dateien liegen unter `/usr/share/cups/model/stp/` und sind durch die Einträge "*NickName: ... CUPS+GimpPrint" und "*cupsFilter: ... rastertoprinter" gekennzeichnet.

PPD-Dateien von Druckerherstellern im Paket manufacturer-PPDs

Das Paket manufacturer-PPDs enthält PPD-Dateien von Druckerherstellern, die unter einer hinreichend freien Lizenz stehen. PostScript-Drucker sollten mit der passenden PPD-Datei des Druckerherstellers eingerichtet werden, denn die PPD-Datei des Druckerherstellers ermöglicht es, alle Funktionen des PostScript-Druckers zu nutzen. YaST verwendet bevorzugt eine PPD-Datei aus manufacturer-PPDs, wenn folgende Bedingungen erfüllt sind:

- Der bei der Hardwareerkennung ermittelte Hersteller- und Modellname stimmt mit dem Hersteller- und Modellnamen in einer PPD-Datei aus manufacturer-PPDs überein.
- Entweder ist die PPD-Datei aus manufacturer-PPDs die einzige zu dem Druckermodell passende PPD-Datei, oder es passt auch eine Foomatic PPD-Datei mit folgendem Eintrag zu dem Druckermodell: "*NickName: ... Foomatic/Postscript (recommended)".

YaST verwendet also in den folgenden Fällen keine PPD-Datei aus manufacturer-PPDs:

- Die PPD-Datei aus manufacturer-PPDs passt hinsichtlich Hersteller- und Modellname nicht. Das kann insbesondere dann passieren, wenn es für ähnliche Modelle nur eine PPD-Datei in manufacturer-PPDs gibt (z. B. wenn bei einer Serie von Modellen nicht für jedes einzelne Modell eine eigene PPD-Datei existiert, sondern als Modellname etwas in der Art wie "Funprinter 1000 series" in der PPD-Datei steht).
- Die Foomatic Postscript PPD-Datei ist aus folgenden Gründen nicht „recommended“: Das Druckermodell arbeitet nicht gut genug im PostScript-Modus (z. B. unzuverlässig weil der Drucker standardmässig zu wenig Speicher hat oder zu langsam weil der Prozessor im Drucker zu leistungsschwach ist) und der Drucker unterstützt PostScript nicht standardmässig (z. B. weil die PostScript-Unterstützung als optionales Modul verfügbar ist).

Wenn für einen PostScript Drucker eine PPD-Datei aus manufacturer-PPDs geeignet ist, aber YaST kann aus obigen Gründen diese nicht einrichten, dann ist das passende Druckermodell manuell in YaST auszuwählen.

13.7 Mögliche Probleme und deren Lösung

13.7.1 Drucker ohne Standarddruckersprache

Ein Drucker, der nur mit speziellen eigenen Steuersequenzen angesprochen werden kann, so hat heißen *GDI-Drucker*. Diese Drucker funktionieren nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber mitliefert. *GDI* ist eine von Microsoft entwickelte Programmierschnittstelle zur grafischen Darstellung. Das Problem ist nicht die Programmierschnittstelle, sondern dass die sog. GDI-Drucker *nur* über die proprietäre Druckersprache des jeweiligen Druckermodells angesprochen werden können.

Es gibt Drucker, die zusätzlich zum GDI-Modus eine Standarddruckersprache verstehen, wozu der Drucker passend einzustellen oder umzuschalten ist. Für einige GDI-Drucker gibt es proprietäre Treiber vom Druckerhersteller. Der Nachteil proprietärer Druckertreiber ist, dass weder garantiert werden kann, dass diese mit dem aktuell installierten Drucksystem funktionieren, noch dass diese für die verschiedenen Hardwareplatformen funktionieren. Drucker, die eine Standarddruckersprache verstehen, sind dagegen weder von einer speziellen Drucksystem-Version noch von einer speziellen Hardwareplatform abhängig.

Es ist in der Regel kostengünstiger, nicht Zeit für die Anpassung eines proprietären Linux-Treiber aufzuwenden, sondern gleich einen unterstützten Drucker anzuschaffen. Insbesondere deswegen nicht, weil mit einem ordentlichen Drucker das Treiberproblem ein für alle Mal gelöst ist. Nie wieder ist dann eine spezielle Treibersoftware einzuspielen und unter Umständen speziell zu konfigurieren und nie wieder müssen Treiber-Updates beschafft werden, wenn das Drucksystem weiterentwickelt wurde.

13.7.2 Geeignete PPD-Datei für PostScript-Drucker fehlt

Wenn für einen PostScript Drucker keine PPD-Datei im Paket manufacturer-PPDs geeignet ist, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden oder eine passende PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (.zip) oder als selbstentpackendes Zip-Archiv (`.exe`) vorliegt, können Sie es mit `unzip` entpacken. Klären Sie zuerst die Lizenzbedingungen der PPD-Datei. Dann testen Sie mit dem Programm `cupstestppd` , ob die PPD-Datei der "Adobe PostScript Printer

Description File Format Specification, Version 4.3" genügt. Wird "FAIL" ausgegeben, dann sind die Fehler in der PPD-Datei so schwerwiegend, dass grössere Probleme zu erwarten sind. Die von `cupstestppd` angegebenen Problemstellen sollten beseitigt werden. Wenn notwendig, fragen Sie direkt den Druckerhersteller nach einer geeigneten PPD-Datei.

13.7.3 Parallel-Ports

Hinweis

Parallel-Ports gibt es nur bei PC-ähnlichen Plattformen.

Hinweis

Am sichersten funktioniert es, wenn der Drucker direkt an der ersten parallelen Schnittstelle angeschlossen ist und im BIOS für die parallele Schnittstelle folgende Einstellungen gesetzt sind:

- IO-Adresse `378` (hexadezimal)
- Interrupt ist nicht relevant
- Modus `Normal`, `SPP` oder `Output-Only`
- DMA wird nicht verwendet

Ist trotz dieser BIOS-Einstellungen der Drucker nicht über die erste parallele Schnittstelle ansprechbar, muss die IO-Adresse entsprechend der BIOS-Einstellung explizit in der Form `0x378` in `/etc/modprobe.conf` eingetragen werden. Sind zwei parallele Schnittstellen vorhanden, die auf die IO-Adressen `378` und `278` (hexadezimal) eingestellt sind, dann sind diese in der Form `0x378,0x278` einzutragen.

Wenn der Interrupt `7` noch frei ist, dann kann mit dem Eintrag in der Datei 13.1 der Interrupt-Betrieb aktiviert werden. Bevor der Interrupt-Betrieb aktiviert wird, ist der Datei `/proc/interrupts` zu entnehmen, welche Interrupts bereits verwendet werden, wobei hier nur die Interrupts angezeigt werden, die momentan in Gebrauch sind. Dies kann sich je nach aktiv benutzter Hardware ändern. Der Interrupt für die parallele Schnittstelle darf nicht anderweitig in Gebrauch sein. Im Zweifel ist der Polling-Betrieb mit `irq=none` zu nehmen.

Beispiel 13.1: */etc/modprobe.conf: Interrupt-Betrieb für die erste parallele Schnittstelle*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

13.7.4 Druckeranschluss via Netzwerk

Netzprobleme nachweisen Schließen Sie den Drucker direkt am Rechner an. Konfigurieren Sie den Drucker zum Test als lokalen Drucker. Wenn es so funktioniert, sind Netzprobleme die Ursache.

TCP/IP-Netzwerk überprüfen Das TCP/IP-Netzwerk inklusive Namensauflösung muss ordnungsgemäß funktionieren.

Einen entfernten lpd prüfen Mit den folgenden Kommando kann man testen, ob überhaupt eine TCP-Verbindung zum lpd (Port `515`) auf dem Rechner ⟨*host*⟩ möglich ist:

```
netcat -z <host> 515 && echo ok || echo failed
```

Wenn keine Verbindung zum lpd möglich ist, dann läuft entweder der lpd nicht, oder grundlegende Netzwerkprobleme sind die Ursache.

Als Benutzer `root` kann man mit folgendem Kommando einen (ggf. sehr langen) Statusbericht für die Warteschlange ⟨*queue*⟩ auf dem (entfernten) Rechner ⟨*host*⟩ abfragen, sofern der dortige lpd läuft und Anfragen dorthin geschickt werden können:

```
echo -e "\004<queue>" \
  | netcat -w 2 -p 722 <host> 515
```

Wenn keine Antwort vom lpd kommt, dann dann läuft entweder der lpd nicht, oder grundlegende Netzwerkprobleme sind die Ursache. Wenn eine Antwort vom lpd kommt, sollte diese klären, warum auf der Warteschlange `queue` auf dem Rechner `host` nicht gedruckt werden kann – Beispiele:

Beispiel 13.2: *Fehlermeldung von lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Wenn eine derartige Antwort vom lpd kommt, liegt das Problem beim entfernten lpd.

Einen entfernten cupsd prüfen Mit folgendem Kommando kann man testen, ob es im Netzwerk einen CUPS-Netzwerk-Server gibt, denn dieser sollte über den UDP Port `631` seine Warteschlange standardmäßig alle 30 Sekunden broadcasten:

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Nach 40 Sekunden Wartezeit sollte es eine Ausgabe in der folgenden Art geben, wenn ein CUPS-Netzwerk-Server broadcastet:

Beispiel 13.3: *Broadcast vom CUPS-Netzwerk-Server*

```
ipp://<host>.<domain>:631/printers/<queue>
```

► **S/390, zSeries**
Beachten Sie, dass die S/390-Ethernet-Karten per Default keine Broadcasts empfangen. ◄

Mit folgendem Kommando testet man, ob überhaupt eine TCP-Verbindung zum cupsd (Port 631) auf dem Rechner ⟨*host*⟩ möglich ist:

```
netcat -z <host> 631 && echo ok || echo failed
```

Wenn keine Verbindung zum cupsd möglich ist, dann läuft entweder der cupsd nicht, oder grundlegende Netzwerkprobleme sind die Ursache.

```
lpstat -h <host> -l -t
```

Damit erhält man einen (ggf. sehr langen) Statusbericht für alle Warteschlangen auf dem Rechner ⟨*host*⟩, sofern der dortige cupsd läuft und Anfragen dorthin geschickt werden können.

```
echo -en "\r" \
  | lp -d <queue> -h <host>
```

Damit kann man testen, ob die Warteschlange ⟨*queue*⟩ auf dem Rechner ⟨*host*⟩ einen Druckauftrag annimmt, wobei der Druckauftrag hier aus einem einzelnen Carriage-Return-Zeichen besteht — d. h. hierbei wird nur getestet, aber normalerweise sollte nichts gedruckt werden — und wenn, dann nur ein leeres Blatt.

Netzwerkdrucker oder Printserver-Box arbeitet nicht zuverlässig

Es gibt mitunter Probleme mit dem Druckerspooler, der in einer Printserver-Box läuft, sobald ein höheres Druckaufkommen vorliegt. Da es am Druckerspooler in der Printserver-Box liegt, kann man das nicht ändern. Man kann aber den Druckerspooler in der Printserver-Box umgehen, indem man den an der Printserver-Box angeschlossenen Drucker direkt via TCP-Socket anspricht.

Dadurch arbeitet die Printserver-Box nur noch als Umwandler zwischen den verschiedenen Formen der Datenübertragung (TCP/IP-Netzwerk und lokaler Druckeranschluss). Dazu muss der entsprechende TCP-Port auf der Printserver-Box bekannt sein. Bei angeschlossenem und eingeschaltetem Drucker an der Printserver-Box kann dieser TCP-Port normalerweise einige Zeit nach dem Einschalten der Printserver-Box mit dem Programm `nmap` aus dem Paket `nmap` ermittelt werden.

So liefert `nmap` ⟨*`IP-address`*⟩ bei einer Printserver-Box beispielsweise:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Diese Ausgabe bedeutet, dass der über den Port `9100` an der Printserver-Box angeschlossene Drucker via TCP-Socket ansprechbar ist. Standardmässig prüft `nmap` nur eine gewisse Liste von allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` verzeichnet sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl: `nmap -p` ⟨*from_port*⟩-⟨*to_port*⟩ ⟨*IP-address*⟩ (das kann dann etwas dauern) — vergleichen Sie dazu die Manual-Page `man nmap`.

Mit Befehlen der Art

```
echo -en "\rHello\r\f" | netcat -w 1 <IP-address> <port>
cat <file> | netcat -w 1 <IP-address> <port>
```

können Zeichenfolgen oder Dateien direkt an den betreffenden Port geschickt werden, um zu testen, ob der Drucker über diesen Port ansprechbar ist.

13.7.5 Fehlerhafte Ausdrucke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag dann komplett abgearbeitet, wenn das CUPS-Backend mit der Datenübertragung zum Empfänger (Drucker) fertig ist. Wenn danach die weitere Verarbeitung beim Empfänger scheitert (z. B. wenn der Drucker die druckerspezifischen Daten nicht zu Papier bringen kann), merkt das Drucksystem davon nichts. Wenn der Drucker die druckerspezifischen Daten nicht zu Papier bringen kann sollte eine andere PPD-Datei gewählt werden, die besser zum Drucker passt.

13.7.6 Abgeschaltete Warteschlangen

Wenn die Datenübertragung zum Empfänger endgültig scheitert (normalerweise macht ein CUPS-Backend mehrere Versuche), meldet das Backend einen Fehler an das Drucksystem (genauer an den cupsd). Das Backend entscheidet, ob und wieviele Versuche sinnvoll sind, bis es die Datenübertragung als unmöglich meldet. Da weitere Versuche somit sinnlos sind, wird das Ausdrucken für die betroffene Warteschlange vom cupsd abgeschaltet (`disable`). Nachdem die Ursache des Problems behoben wurde, muss der Systemverwalter mit `/usr/bin/enable` das Ausdrucken wieder aktivieren.

13.7.7 Löschen von Druckaufträgen bei CUPS-Browsing

Wenn ein CUPS-Netzwerk-Server seine Warteschlangen via Browsing den Client-Rechnern mitteilt und auf den Client-Rechnern läuft dazu passend ein lokaler cupsd, dann nimmt der cupsd des Clients die Druckaufträge von den Anwendungsprogrammen an und schickt sie sofort weiter an den cupsd des Servers. Wenn ein cupsd einen Druckauftrag annimmt, bekomt er immer eine neue Job-Nummer. Daher ist die Job-Nummer auf dem Client-Rechner eine andere als auf dem Server. Da ein Druckauftrag sofort weitergeschickt wird, kann er normalerweise nicht mit der Job-Nummer des Client-Rechners gelöscht werden, denn für den cupsd des Clients ist der Druckauftrag mit der erfolgreichen Weiterleitung an den cupsd des Servers komplett abgearbeitet (siehe oben). Um den Druckauftrag auf dem Server zu löschen, ist z. B. mit folgendem Befehl die Job-Nummer auf dem Server zu ermitteln, sofern der Server den Druckauftrag nicht auch schon abgearbeitet (d.h. an den Drucker geschickt) hat:

```
lpstat -h <print-server> -o
```

Dann kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h <print-server> <warteschlange>-<jobnummer>
```

13.7.8 Druckaufträge fehlerhaft oder Datentransfer gestört

Druckaufträge bleiben in den Warteschlangen erhalten und werden ggf. von Anfang an erneut gedruckt, wenn Sie während eines Druckvorgangs den Drucker aus- und einschalten oder den Rechner herunterfahren und neu starten. Einen fehlerhaften Druckauftrag müssen Sie mit dem `cancel` Befehl aus der Warteschlange entfernen.

Ist ein Druckauftrag fehlerhaft oder kommt es zu einer Störung in der Kommunikation zwischen Rechner und Drucker, kann der Drucker mit den gesendeten Daten nichts Sinnvolles anfangen. Es werden lediglich Unmengen Papier mit sinnlosen Zeichen bedruckt.

1. Entnehmen Sie zuerst alles Papier bei Tintenstrahldruckern bzw. öffnen Sie die Papierschächte bei Laserdruckern, damit das Drucken aufhört. Bei hochwertigen Druckern gibt es am Drucker einen Knopf, den aktuellen Ausdruck abzubrechen.

2. Da der Druckauftrag erst dann aus der Warteschlange entfernt wird, nachdem er komplett an den Drucker geschickt wurde, wird er meist noch in der Warteschlange stehen. Prüfen Sie mit `lpstat -o` (bzw. mit `lpstat -h` ⟨*print-server*⟩ `-o`) aus welcher Warteschlange gerade gedruckt wird und löschen Sie mit `cancel` ⟨*warteschlange*⟩`-`⟨*jobnummer*⟩ (bzw. mit `cancel -h` ⟨*print-server*⟩ ⟨*warteschlange*⟩`-`⟨*jobnummer*⟩) den Druckauftrag. Unter KDE stehen auch die Programme kprinter oder kjobviewer für diese Zwecke zur Verfügung.

3. Eventuell werden noch einige Daten an den Drucker übertragen, obwohl der Druckauftrag aus der Warteschlange gelöscht ist. Prüfen Sie ob noch ein CUPS-Backend Prozess für die betreffende Warteschlange läuft und beenden Sie diesen. Z.B. können für einen Drucker am Parallelport mit dem Befehl `fuser -k /dev/lp0` alle Prozesse beendet werden, die noch auf den Drucker (genauer: den Parallelport) zugreifen.

4. Setzen Sie den Drucker komplett zurück, indem Sie ihn einige Zeit vom Stromnetz trennen. Danach legen Sie das Papier wieder ein und schalten den Drucker an.

13.7.9 Ursachen für Probleme im CUPS-Drucksystem

1. Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.
2. Stoppen Sie den cupsd.
3. Bewegen Sie `/var/log/cups/error_log*` weg damit Sie nicht in zu grossen Logdateien suchen müssen.
4. Starten Sie den cupsd.
5. Versuchen Sie erneut, was zu dem Problem geführt hat.
6. Nun finden sich viele Meldungen in `/var/log/cups/error_log*`, die zur Ursachenermittlung nützlich sind.

Das Hotplug-System

Das Hotplug-System unter SUSE LINUX geht zurück auf das *Linux Hotplug Project*, unterscheidet sich allerdings in Teilen. Der Hauptunterschied besteht darin, dass unter SUSE LINUX nicht der Event Multiplexer `/etc/hotplug.d` benutzt wird, sondern die Skripte `/sbin/hwup` und `/sbin/hwdown`, um Hotplug-Geräte (*engl. devices*) zu initialisieren oder zu stoppen.

► **S/390, zSeries**
Viele der hier beschriebenen Hard- und Softwareeigenschaften, die in diesem Kapitel zu finden sind, existieren so nicht auf IBM S/390 und zSeries.
◄

14.1 Geräte und Schnittstellen 348
14.2 Hotplug Events 349
14.3 Hotplug Agenten 349
14.4 Automatisches Laden von Modulen 350
14.5 Netzwerkgeräte und Schnittstellenbezeichnungen 351
14.6 Hotplug mit PCI 351
14.7 Coldplug 352
14.8 Fehleranalyse 352

Das Hotplug-System wird nicht nur für Geräte verwendet, die während des Betriebs ein- und ausgesteckt werden können, sondern für alle Geräte, die erst nach dem Booten des Kernels erkannt werden. Diese Geräte sind im `sysfs` Dateisystem eingetragen, das unter `/sys` eingehängt ist. Vor dem Booten des Kernels werden nur absolut notwendige Geräte wie Bussystem, Bootdisketten oder Tastatur initialisiert.

Die wichtigsten Hotplug-Funktionen konfigurieren Sie in zwei Dateien: In `/etc/sysconfig/hotplug` finden Sie Variablen, die das Verhalten von `hotplug` und `coldplug` beeinflussen. Jede Variable wird durch einen Kommentar erklärt. Die Datei `/proc/sys/kernel/hotplug` enthält den Namen des ausführbaren Programs, das vom Kernel aufgerufen wird.

14.1 Geräte und Schnittstellen

Neben Geräten werden auch Schnittstellen über das Hotplug-System verwaltet. Ein Gerät ist entweder mit einem Bus oder einer Schnittstelle verbunden; eine Schnittstelle verbindet Geräte miteinander oder mit einer Anwendung.

Geräte, die in `sysfs` eingetragen sind, findet man unter `/sys/devices`, Schnittstellen liegen unter `/sys/class` oder `/sys/block`. Alle Schnittstellen sollten in der Datei `sysfs` eine Verknüpfung (*engl. link*) auf ihr Gerät eintragen, aber es gibt noch immer einige Treiber, die diesen Link nicht automatisch hinzufügen.

Typische Beispiele für Geräte und Schnittstellen sind beispielsweise:

PCI-Netzwerkkarte Ein Gerät, das mit dem PCI-Bus verbunden ist (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`) und über eine Netzwerk-Schnittstelle verfügt, die von Netzwerkdiensten benutzt wird oder mit einem virtuellen Netzwerkgerät wie einem Tunnel oder vlan verbunden ist. (`/sys/class/net/eth0`).

PCI SCSI Controller Ein Gerät (`/sys/devices/pci0000:20/0000:20:01.1`), das mehrere physikalische Schnittstellen in Form eines Buses (`/sys/class/scsi_host/host1`) zur Verfügung stellt.

SCSI Festplatte Ein Gerät (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0`) mit mehreren Schnittstellen (`/sys/block/sda*`).

14.2 Hotplug Events

Für jedes Gerät und jede Schnittstelle gibt es einen sogenannten Hotplug Event, der vom entsprechenden Hotplug Agenten verarbeitet wird. Hotplug Events werden entweder vom Kernel ausgelöst, wenn eine Verbindung zu einem Gerät hergestellt wird, oder von *coldplug*, das regelmäßig wichtige Busse prüft und für alle nicht initialisierten Geräte einen Event erzeugt. Mehr zu *coldplug* erfahren Sie im Abschnitt 14.7 auf Seite 352. Darüber hinaus löst der Kernel einen Hotplug Event aus, sobald ein Treiber eine Schnittstelle registriert.

Ein Hotplug Event ist der Aufruf eines Hotplug Usermode Tools wie `/sbin/hotplug`, das in der Datei `/proc/sys/kernel/hotplug` spezifiziert ist. `/sbin/hotplug` sucht nach einem Hotplug Agenten, der dem Typ des Events entspricht. Gibt es keinen passenden Agenten aber eine Datei `dev` im Gerätepfad, wird der Agent generic_udev.agent aufgerufen.

Hinweis

Sollen Events bestimmter Art grundsätzlich ignoriert werden, editieren Sie dazu die Datei `/etc/sysconfig/hotplug` und setzen die gewünschten Event auf `HOTPLUG_SKIP_EVENTS`.

Hinweis

14.3 Hotplug Agenten

Mit Kernel 2.6 sind viele verschiedene Hotplug Events neu dazugekommen. Jeder neue Treiber kann einen neuen Event einführen. Nur für die bereits bekannten Events gibt es einen zugeordneten Agenten, der die notwendige Aktion ausführt.

Geräte-Agenten laden überwiegend Kernelmodule, müssen allerdings gelegentlich auch zusätzliche Befehle aufrufen. Beispielsweise muss bei einigen Rechner-Architekturen wie IBM S390 jedes Gerät einen bestimmten Wert in `procfs` oder `sysfs` schreiben, um initialisiert zu werden. Unter SUSE LINUX kümmert sich darum `/sbin/hwup` beziehungsweise `/sbin/hwdown`. Diese Programme suchen in der Datei `/etc/sysconfig/hardware` nach einer Konfiguration, die zum Gerät passt. Findet `/sbin/hwup` keine Konfiguration, werden automatisch Module geladen. Mehr dazu erfahren Sie unter 14.4. Informationen zu `/sbin/hwup`

finden Sie in der Datei /usr/share/doc/packages/sysconfig/README und in der Manualpage mit man hwup.

Schnittstellen-Agenten übernehmen in erste Linie zwei Aufgaben: Sie initialisieren die Schnittstelle oder rufen udev auf, um eine Geräte-Verknüpfung (*engl. device node*) zu erzeugen. Netzwerk-Schnittstellen werden mit /sbin/ifup initialisiert und mit /sbin/ifdown deaktiviert. Details dazu finden Sie in der Datei /usr/share/doc/packages/sysconfig/README und in der Manual Page mit dem Befehl man ifup. Auch zu udev gibt es eine Manual page, die Sie mit man udev lesen können. Beachten Sie dazu auch den Abschnitt 15 auf Seite 355.

14.4 Automatisches Laden von Modulen

Konnte ein Gerät nicht mit /sbin/hwup initialisiert werden, durchsucht der Agent sogenannte „Module Maps“ nach einem passenden Treiber. Die erste Wahl sind dabei die Maps in /etc/hotplug/*.handmap, wird er nicht fündig, sucht er auch in /lib/modules/<kernelversion>/modules.*map. Wollen Sie einen anderen Treiber benutzen als den Standard-Treiber des Kernels, tragen Sie diesen in /etc/hotplug/*.handmap ein, da diese Datei zuerst eingelesen wird.

Beachten Sie dabei bitte die folgenden Unterschiede zwischen USB und PCI. Der Agent usb.agent sucht auch noch in den Dateien /etc/hotplug/usb.usermap und /etc/hotplug/usb/*.usermap nach Usermode-Treibern. Auf diese Weise kann man ausführbare Programme für bestimmte Geräte aufrufen.

Bei PCI-Geräten frägt pci.agent zunächst bei hwinfo nach Treiber-Modulen an. Nur wenn hwinfo keinen Treiber kennt, sieht der Agent in der pci.handmap und der Kernelmap nach, was allerdings vor ihm schon hwinfo getan hat und deshalb ebenfalls scheitern muss. hwinfo verfügt über eine zusätzliche Datenbank, die nach der Handmap und vor der Kernelmap eingelesen wird.

Der Agent pci.agent kann auf Treiber-Module in einem bestimmten Unterverzeichnis von /lib/modules/<kernelversion>/kernel/drivers eingeschränkt werden. Spezifizieren Sie dieses oder mehrere Verzeichnisse in der Datei /etc/sysconfig/hotplugmit der Variable HOTPLUG_PCI_DRIVERTYPE_WHITELIST. Im Gegensatz dazu können Sie auch Verzeichnisse ausschließen, indem Sie diese bei HOTPLUG_-

PCI_DRIVERTYPE_BLACKLIST angeben. Die Module in diesen Verzeichnissen werden niemals geladen. Darüber hinaus können Sie in der Datei /etc/hotplug/blacklist Module eintragen, die niemals von einem Agenten geladen werden dürfen. Schreiben Sie jeden Modulnamen in eine eigene Zeile.

Werden mehrere passende Module in einer Mapdatei gefunden, wird nur das erste Modul geladen. Wünschen Sie, dass alle Module geladen werden, setzen Sie die Variable HOTPLUG_LOAD_MULTIPLE_MODULES=yes.

Hinweis

Module, die mit hwup geladen werden, betrifft dies nicht. Automatisches Laden von Modulen tritt nur in Ausnahmefällen ein.

Hinweis

14.5 Netzwerkgeräte und Schnittstellenbezeichnungen

Verfügt ein Rechner über mehrere Netzwerkgeräte mit unterschiedlichen Treibern, kann es passieren, dass sich nach dem Booten die Schnittstellenbezeichnungen ändern, falls dieses Mal ein anderer Treiber schneller geladen wurde. Aus diesem Grund werden in SUSE LINUX Netzwerkgeräte über eine Warteschlange verwaltet. Dieses Verhalten können Sie in der Datei /etc/sysconfig/hotplug über die Variable HOTPLUG_PCI_QUEUE_NIC_EVENTS=no abstellen.

Der bessere Weg zu konsistenten Schnittstellenbezeichnungen besteht allerdings darin, in den Konfigurationsdateien der einzelnen Schnittstellen den gewünschten Namen anzugeben. Details zu dieser Methode finden Sie in der Datei /usr/share/doc/packages/sysconfig/README.

14.6 Hotplug mit PCI

Einige Rechner ermöglichen Hotplug auch für PCI-Geräte. Um dies voll zu nutzen, müssen besondere Kernel-Module geladen werden, die auf

nicht-PCI Hotplug-Rechnern Schaden anrichten können. Hotplug PCI-Steckplätze können leider nicht automatisch erkannt werden, daher müssen Sie diese Funktion manuell konfigurieren. Setzen Sie dazu die Variable `HOTPLUG_DO_REAL_PCI_HOTPLUG` in der Datei `/etc/sysconfig/hotplug`.

14.7 Coldplug

Coldplug ist zuständig für alle Geräte, die bereits angeschlossen sind, bevor das Hotplug-System während des Bootvorgangs aktiviert wird. Es kümmert sich auch um Geräte, die nicht leicht zu erkennen sind.

Zunächst ruft das Skript `rccoldplug` für jede statische Hardware Konfiguration `/etc/sysconfig/hardware/hwcfg-static-*` den Befehl `hwup` auf. Anschließend suchen die Skripte `/etc/hotplug/*.rc` nach Geräten, die noch nicht initialisiert sind und erzeugen Hotplug Events. Für PCI-Geräte gibt es eine Positiv- und eine Negativliste von Geräte-Typen, die `coldplug` initialisieren oder überspringen soll. In der Datei `/etc/sysconfig/hotplug` gibt es dazu ausführliche Kommentare.

Die Scan-Skripten geben für jedes geprüfte Gerät einen Buchstaben auf dem Bildschirm aus:

. Gerät ist bereits initialisiert und wird übersprungen.

***** Hotplug Event für das Gerät wird erzeugt.

W Gerät befindet sich nicht auf der Whitelist und wird übersprungen.

B Gerät steht auf der Blacklist und wird übersprungen.

14.8 Fehleranalyse

14.8.1 Protokoll-Dateien

Standardmäßig schickt `hotplug` nur einige wichtige Nachrichten an `syslog`. Um mehr Informationen zu erhalten, setzen Sie die Variable `HOTPLUG_DEBUG=yes`. Wenn Sie diese Variable auf den Wert `max` setzen, wird jedes Shell-Kommando aller Hotplug-Skripten protokolliert. Entsprechend groß wird die Datei `/var/log/messages`, in der `syslog` alle Nachrichten speichert. Da `syslog` während des Bootens erst nach

hotplug und coldplug gestartet wird, können allerdings die ersten Meldungen noch nicht protokolliert werden. Sind diese Meldungen wichtig für Sie, setzen Sie über die Variable HOTPLUG_SYSLOG eine andere Protokoll-Datei. Beachten Sie dazu die Kommentare in /etc/sysconfig/hotplug.

14.8.2 Boot-Probleme

Falls ein Rechner beim Booten hängen bleibt, können Sie hotplug oder coldplug deaktivieren, indem Sie am Bootprompt NOHOTPLUG=yes beziehungsweise NOCOLDPLUG=yes eingeben. Im laufenden System können Sie Hotplug wieder aktivieren, indem Sie den Befehl rchotplug start eingeben.

Um herauszufinden, ob ein bestimmtes Modul, das von hotplug geladen wird, für die Probleme verantwortlich ist, geben Sie am Bootprompt HOTPLUG_TRACE=<N> ein. Die Namen aller Module werden nacheinander am Bildschirm ausgegeben, bevor sie nach N Sekunden tatsächlich geladen werden. Sie können hier nicht interaktiv eingreifen.

14.8.3 Der Event-Recorder

Das Skript /sbin/hotplugeventrecorder wird bei jedem Event von von /sbin/hotplug und sbin/hotplug-stopped aufgerufen. Wenn ein Verzeichnis /events existiert, werden alle Hotplug Events als einzelne Dateien in diesem Verzeichnis abgelegt.

Dynamische Device Nodes mit udev

Mit Linux Kernel 2.6 gibt es eine neue *Userspace* Lösung für ein dynamisches Geräte-Verzeichnis `/dev` mit konsistenten Geräte-Bezeichnungen: `udev`. Die Vorgänger-Implementierung von `/dev` mit `devfs` funktioniert nicht mehr und wird von `udev` ersetzt.

15.1 Grundlagen zum Erstellen von Regeln 356
15.2 Automatisierung bei NAME und SYMLINK 357
15.3 Reguläre Ausdrücke in Schlüsseln 357
15.4 Tipps zur Auswahl geeigneter Schlüssel 358
15.5 Konsistente Namen für Massen-Speichergeräte . . 359

Traditionellerweise wurden auf Linux-Systemen im Verzeichnis `/dev` Geräte-Verknüpfungen (*engl. device nodes*) gespeichert. Für jede mögliche Art von Gerät gab es eine Verknüpfung, unabhängig davon, ob es im System tatsächlich existierte. Entsprechend groß wurde dieses Verzeichnis. Mit `devfs` trat eine deutliche Verbesserung ein, denn nur noch real existierende Geräte erhielten einen Device Node in `/dev`.

`udev` geht einen neuen Weg bei der Erzeugung der Device Nodes. Es vergleicht Informationen, die `sysfs` zur Verfügung stellt, mit Angaben des Benutzers in Form von Regeln. `sysfs` ist ein neues Dateisystem des Kernels 2.6 und stellt die grundlegenden Informationen über angeschlossene Geräte im System zur Verfügung. Es wird unter `/sys` eingehängt.

Die Erstellung von Regeln durch den Benutzer ist nicht zwingend erforderlich. Wird ein Gerät angeschlossen, wird auch die entsprechende Geräteverknüpfung erzeugt. Allerdings bieten die Regeln die Möglichkeit, die Namen der Verknüpfungen zu ändern. Dies bietet den Komfort, einen kryptischen Gerätenamen durch einen leicht zu merkenden zu ersetzen und darüber hinaus konsistente Gerätenamen zu erhalten, wenn man zwei Geräte des gleichen Typs angeschlossen hat.

Zwei Drucker erhalten standardmäßig die Bezeichnungen `/dev/lp0` und `/dev/lp1`. Welches Gerät welchen Device Node erhält hängt allerdings von der Reihenfolge ab, in der sie eingeschaltet werden. Ein weiteres Beispiel sind externe Massenspeichergeräte wie USB-Festplatten. Mit `udev` lassen sich exakte Geräte-Pfade in `/etc/fstab` eintragen.

15.1 Grundlagen zum Erstellen von Regeln

Bevor `udev` Geräte-Verknüpfungen unter `/dev` erzeugt, liest es die Datei `/etc/udev/udev.rules` ein. Die erste Regel, die zu einem Gerät passt, wird verwendet, auch wenn noch weitere existieren sollten. Kommentare werden mit einem Hash-Zeichen (#) eingeleitet. Regeln haben die Form:

```
Schlüssel, [Schlüssel,...] NAME [, SYMLINK]
```

Mindestens ein Schlüssel muss angegeben werden, da über diesen die Regel einem Gerät zugeordnet wird. Auch der Name ist zwingend erforderlich, denn unter diesem Namen wird die Geräte-Verknüpfung in `/dev`

angelegt. Der optionale Symlink-Parameter erlaubt es Verknüpfungen an weiteren Stellen anzulegen. Eine Regel für einen Drucker könnte also folgendermaßen aussehen:

```
BUS="usb", SYSFS{serial}="12345", NAME="lp_hp", SYMLINK="printers/hp"
```

In diesem Beispiel gibt es zwei Schlüssel: BUS und SYSFSserial. `udev` wird die Seriennummer mit der des Geräts, das an den USB-Bus angeschlossen ist, verglichen. Alle Schlüssel müssen übereinstimmen, um dem Gerät den Namen `lp_hp` im Verzeichnis `/dev` zuzuweisen. Darüber hinaus wird es einen symbolischen `/dev/printers/hp` anlegen, der auf die Geräte-Verknüpfung verweist. Das Verzeichnis `printers` wird dabei automatisch erzeugt. Druckaufträge können danach an `/dev/printers/hp` oder `/dev/lp_hp` geschickt werden.

15.2 Automatisierung bei NAME und SYMLINK

Die Parameter NAME und SYMLINK erlauben die Verwendung von Operatoren zur Automatisierung von Zuweisungen. Diese Operatoren beziehen sich auf Kernel-Daten über das entsprechende Gerät. Zur Veranschaulichung dient ein einfaches Beispiel:

```
BUS="usb", SYSFS{vendor}="abc", SYSFS{model}="xyz", NAME="camera%n"
```

Der Operator %n wird im Namen durch die Nummer für das Kamera-Device ersetzt: `camera0`, `camera1`, etc. Ein weiterer nützlicher Operator ist %k, der durch den Standard-Gerätenamen des Kernels ersetzt wird, zum Beispiel `hda1`. In der Manualpage von `udev` finden Sie eine Liste aller Operatoren.

15.3 Reguläre Ausdrücke in Schlüsseln

In den Schlüsseln können reguläre Ausdrücke wie die Wildcards (Jokerzeichen) in der Shell verwendet werden, so zum Beispiel das Zeichen * als Platzhalter für beliebige Zeichen oder ? für genau ein beliebiges Zeichen.

```
KERNEL="ts*", NAME="input/%k"
```

Mit dieser Regel erhält ein Gerät, dessen Bezeichnung mit den Buchstaben "ts" beginnt, den Standard-Kernelnamen im Standard-Verzeichnis. Detaillierte Informationen zum Gebrauch von regulären Ausdrücken in udev-Regeln entnehmen Sie bitte der Manualpage `man udev`.

15.4 Tipps zur Auswahl geeigneter Schlüssel

Die Wahl eines guten Schlüssels ist Voraussetzung für jede funktionierende udev-Regel. Standardschlüssel sind beispielsweise:

BUS Bustyp des Geräts

KERNEL Gerätename, den der Kernel benutzt

ID Gerätenummer auf dem Bus (z.B. PCI-Bus ID)

PLACE Physikalische Stelle an der das Gerät angeschlossen ist (z.B. bei USB)

Die Schlüssel ID und Place können sich als nützlich erweisen, allerdings werden meist die Schlüssel BUS und KERNEL sowie SYSFS... benutzt. Darüber hinaus stellt `udev` Schlüssel bereit, die externe Skripte aufrufen und deren Ergebnis auswerten. Ausführliche Informationen dazu finden Sie in der Manualpage `man udev`.

`sysfs` legt kleine Dateien mit Hardware-Informationen in einem Verzeichnisbaum ab. Dabei enthält jede Datei in der Regel nur eine Information wie den Gerätenamen, den Hersteller oder die Seriennummer. Jede dieser Dateien kann als Schlüsselwert verwendet werden. Wollen Sie mehrere SYSFS... Schlüssel in einer Regel verwenden, dürfen Sie allerdings nur Dateien im selben Verzeichnis verwenden.

udevinfo erweist sich hier als nützliches Werkzeug. Sie müssen unter `/sys` nur ein Verzeichnis finden, das sich auf das entsprechende Gerät bezieht und eine Datei `dev` enthält. Diese Verzeichnisse finden sich alle unter `/sys/block` oder `/sys/class`.

Falls bereits ein Device Node für das Gerät existiert, kann Ihnen `udevinfo` auch hier die Arbeit abnehmen. Der Befehl `udevinfo -q path -n /dev/sda` gibt `/block/sda` aus. Das bedeutet, das gesuchte Verzeichnis ist `/sys/block/sda`. Rufen Sie anschließend `udevinfo` mit folgendem

Befehl `udevinfo -a -p /sys/block/sda` auf. Die beiden Befehle können auch kombiniert werden: `udevinfo -a -p ‘udevinfo -q path -n /dev/sda‘`. Ein Ausschnitt der Ausgabe sieht etwa so aus:

```
BUS="scsi"
ID="0:0:0:0"
SYSFS{detach_state}="0"
SYSFS{type}="0"
SYSFS{max_sectors}="240"
SYSFS{device_blocked}="0"
SYSFS{queue_depth}="1"
SYSFS{scsi_level}="3"
SYSFS{vendor}="        "
SYSFS{model}="USB 2.0M DSC    "
SYSFS{rev}="1.00"
SYSFS{online}="1"
```

Suchen Sie sich aus der gesamten Ausgabe und Fülle von Informationen passende Schlüssel aus, die sich nicht ändern werden. Denken Sie daran, dass Sie Schlüssel aus verschiedenen Verzeichnissen nicht in einer Regel verwenden dürfen.

15.5 Konsistente Namen für Massen-Speichergeräte

Mit SUSE LINUX werden Skripte ausgeliefert, die Sie dabei unterstützen, Festplatten und anderen Speichergeräten immer dieselben Bezeichnungen zuzuordnen. `/sbin/udev.get_persistent_device_name.sh` ist ein Wrapper-Skript. Es ruft zunächst `/sbin/udev.get_unique_hardware_path.sh` auf, das den Hardware-Pfad zu einem angegebenen Gerät ermittelt. Außerdem erfrägt `/sbin/udev.get_unique_drive_id.sh` die Seriennummer. Beide Ausgaben werden and `udev` übergeben, das symbolische Links zum Device Node unter `/dev` erzeugt. Das Wrapperskript kann direkt in den udev-Regeln verwendet werden. Ein Beispiel für SCSI, das auch auf USB oder IDE übertragen werden kann (bitte in einer Zeile angeben):

```
BUS="scsi", PROGRAM="/sbin/udev.get_persistent_device_name.sh",
NAME="%k" SYMLINK="%c{1+}"
```

Sobald ein Treiber für ein Massenspeichergerät geladen wurde, meldet er sich mit allen vorhandenen Festplatten beim Kernel an. Jede von ihnen wird einen Hotplug Block-Event auslösen, der `udev` aufruft. `udev` liest zunächst die Regeln ein, um festzustellen, ob ein Symlink erzeugt werden muss.

Wenn der Treiber über die `initrd` geladen wird, gehen die Hotplug-Events verloren. Allerdings sind alle Informationen in `sysfs` gespeichert. Das Hilfsprogramm `udevstart` findet alle Device Dateien unter `/sys/block` und `/sys/class` und startet `udev`.

Darüber hinaus gibt es ein Startskript `boot.udev`, das während des Bootens alle Device Nodes neu erzeugt. Das Startskript muss allerdings über den YaST Runlevel Editor oder mit dem Befehl `insserv boot.udev` aktiviert werden.

Hinweis

Es gibt eine Reihe von Werkzeugen und Programmen, die sich fest darauf verlassen, dass `/dev/sda` eine SCSI-Festplatte und `/dev/hda` eine IDE-Platte ist. Wenn dies nicht der Fall ist, funktionieren diese Programme nicht mehr. YaST ist allerdings auf diese Werkzeuge angewiesen und arbeitet deshalb nur mit den Kernel Gerätebezeichnungen.

Hinweis

Mobiles Arbeiten unter Linux

Dieses Kapitel befasst sich mit den Besonderheiten des mobilen Arbeitens — schwerpunktmäßig auf Notebooks — unter Linux. Die Konfiguration von PC-Karten (PCMCIA) wird ebenso behandelt wie die Verwaltung verschiedener Systemprofile mittels SCPM und die drahtlose Kommunikation mittels IrDA und Bluetooth.

► **S/390, zSeries**
Die in diesem Kapitel beschriebenen Hardware-Spezifika existieren auf IBM S/390 und zSeries nicht. Das Kapitel ist für diese Plattformen nicht relevant. ◄

16.1 PCMCIA 362
16.2 SCPM – System Configuration Profile Management 373
16.3 IrDA – Infrared Data Association 381
16.4 Bluetooth – Geräte drahtlos verbinden 384

16.1 PCMCIA

PCMCIA steht für *Personal Computer Memory Card International Association* und wird als Sammelbegriff für sämtliche damit zusammenhängende Hard- und Software verwendet.

16.1.1 Die Hardware

Die wesentliche Komponente ist die PCMCIA-Karte; hierbei unterscheidet man zwei Typen:

PC-Karten Das sind die derzeit noch am häufigsten vorkommenden Karten. Sie verwenden einen 16 Bit breiten Bus zur Datenübertragung, sind meist relativ günstig und werden in der Regel problemlos und stabil unterstützt.

CardBus-Karten Diese Karten bilden einen neueren Standard. Sie verwenden einen 32 Bit breiten Bus, sind dadurch schneller, aber auch teurer. Da die Datenübertragungsrate aber häufig an anderer Stelle eingeschränkt wird, lohnt sich der Aufwand oft nicht. Es gibt mittlerweile auch für diese Karten etliche Treiber, wobei manche immer noch instabil sind – abhängig auch vom vorhandenen PCMCIA-Controller.

Welche Karte eingesteckt ist, sagt bei aktivem PCMCIA-Dienst das Kommando `cardctl ident`. Eine Liste von unterstützten Karten findet man in `SUPPORTED.CARDS` im Verzeichnis `/usr/share/doc/packages/pcmcia/`. Dort gibt es auch die jeweils aktuelle Version des PCMCIA-HOWTO.

Die zweite notwendige Komponente ist der PCMCIA-Controller oder auch die PC-Card/CardBus-Bridge. Diese stellt die Verbindung zwischen der Karte und dem PCI-Bus her, in älteren Geräten auch die Verbindung zum ISA-Bus. Diese Controller sind fast immer zum Intel-Chip i82365 kompatibel; es werden alle gängigen Modelle unterstützt. Der Typ des Controllers lässt sich mit dem Kommando `pcic_probe` ermitteln. Falls es ein PCI-Gerät ist, gibt das Kommando `lspci -vt` weitere Auskünfte.

16.1.2 Die Software

Unterschiede zwischen beiden PCMCIA-Systemen

Gegenwärtig gibt es zwei PCMCIA-Systeme: externes PCMCIA und Kernel-PCMCIA. Das externe PCMCIA-System von David Hinds ist das

ältere, somit auch besser erprobte, und es wird immer noch weiterentwickelt. Die Quellen der verwendeten Module sind nicht in die Kernelquellen integriert, deshalb die Bezeichnung „externes“ System. Seit Kernel 2.4 gibt es alternative Module in den Kernelquellen. Diese bilden das PCMCIA-System des Kernels („Kernel-PCMCIA“). Die Basismodule wurden von Linus Torvalds geschrieben und unterstützen vor allem neuere CardBus-Bridges effektiver.

Leider sind diese beiden Systeme zueinander inkompatibel. Außerdem gibt es in beiden Systemen unterschiedliche Sätze von Kartentreibern. Deswegen kommt je nach verwendeter Hardware nur ein System in Frage. Die Voreinstellung unter SUSE LINUX ist das neuere Kernel-PCMCIA. Es ist jedoch möglich, das System zu wechseln. Dazu muss in der Datei `/etc/sysconfig/pcmcia` der Variablen `PCMCIA_SYSTEM` entweder der Wert `external` oder `kernel` zugewiesen und PCMCIA mit `rcpcmcia restart` neu gestartet werden. Für vorübergehende Wechsel können Sie auch `rcpcmcia [re]start external,kernel` verwenden. Detailinformationen dazu befindet sich in `/usr/share/doc/packages/pcmcia/LIESMICH.SuSE`.

Die Basismodule

Die Kernelmodule für beide Systeme befinden sich in den Kernelpaketen. Zusätzlich werden noch die Pakete `pcmcia` und `hotplug` benötigt.

Beim Start von PCMCIA werden die Module `pcmcia_core`, `i82365` (externes PCMCIA) oder `yenta_socket` (Kernel-PCMCIA) und `ds` geladen. In sehr seltenen Fällen wird alternativ zu `i82365` bzw. `yenta_socket` das Modul `tcic` benötigt. Sie initialisieren die vorhandenen PCMCIA-Controller und stellen Basisfunktionen zur Verfügung.

Der Cardmanager

Da PCMCIA-Karten zur Laufzeit gewechselt werden können, muss es einen Daemonen geben, der die Aktivitäten in den Steckplätzen überwacht. Diese Aufgabe erledigen je nach gewähltem PCMCIA-System und verwendeter Hardware der Cardmanager oder das Hotplug-System des Kernels. Bei externem PCMCIA kommt nur der Cardmanager zum Einsatz. Bei Kernel-PCMCIA handhabt der Cardmanager nur die PC-Card-Karten, wohingegen CardBus-Karten von Hotplug behandelt werden. Der Cardmanager wird vom PCMCIA-Startskript nach dem Laden der Basismodule gestartet. Da Hotplug neben PCMCIA auch noch andere Subsysteme bedient, gibt es hierfür ein eigenes Startskript.

Ist eine Karte eingeschoben, ermittelt der Cardmanager bzw. Hotplug Typ und Funktion und lädt die passenden Module. Wurden diese erfolgreich geladen, startet der Cardmanager bzw. Hotplug je nach Funktion der Karte bestimmte Initialisierungsskripten, die ihrerseits die Netzwerkverbindung aufbauen, Partitionen von externen SCSI-Platten einhängen (mounten) oder andere hardwarespezifische Aktionen ausführen. Die Skripte des Cardmanagers befinden sich in `/etc/pcmcia/`. Die Skripte für Hotplug sind in `/etc/hotplug/` zu finden. Wenn die Karte wieder entfernt wird, beendet der Cardmanager bzw. Hotplug mit den selben Skripten sämtliche Kartenaktivitäten. Anschließend werden die nicht mehr benötigten Module wieder entladen.

Sowohl der Startvorgang von PCMCIA als auch die Kartenereignisse werden in der Systemprotokolldatei (`/var/log/messages`) protokolliert. Dort wird festgehalten, welches PCMCIA System gerade verwendet wird und welcher Daemon welche Skripte zur Einrichtung verwendet hat. Theoretisch kann eine PCMCIA-Karte einfach entnommen werden. Dies funktioniert auch hervorragend für Netzwerk-, Modem- oder ISDN-Karten, solange keine aktiven Netzwerkverbindungen mehr bestehen. Es funktioniert nicht im Zusammenhang mit eingehängten Partitionen einer externen Platte oder mit NFS-Verzeichnissen. Hier müssen Sie dafür sorgen, dass die Einheiten synchronisiert und sauber ausgehängt werden (unmounten). Das ist natürlich nicht mehr möglich, wenn die Karte bereits herausgenommen wurde. Im Zweifelsfall hilft ein `cardctl eject`.

Dieser Befehl deaktiviert alle Karten, die sich noch im Notebook befinden. Um nur eine der Karten zu deaktivieren, können Sie zusätzlich die Slotnummer angeben, zum Beispiel `cardctl eject 0`.

16.1.3 Die Konfiguration

Ob PCMCIA bzw. Hotplug beim Booten gestartet wird, lässt sich mit dem Runleveleditor von YaST oder auf der Kommandozeile mittels `chkconfig` einstellen.

In `/etc/sysconfig/pcmcia` befinden sich vier Variablen:

`PCMCIA_SYSTEM` bestimmt, welches PCMCIA-System verwendet wird.

`PCMCIA_PCIC` enthält den Namen des Moduls, das den PCMCIA-Controller ansteuert. Im Normalfall ermittelt das Startskript diesen Namen selbstständig. Nur wenn dies fehlschlägt, kann das Modul hier eingetragen werden. Ansonsten sollte diese Variable leer bleiben.

PCMCIA_CORE_OPTS ist für Parameter für das Modul `pcmcia_core` gedacht; sie werden aber nur selten benötigt. Diese Optionen sind in der Manualpage von `pcmcia_core` beschrieben.

PCMCIA_PCIC_OPTS nimmt Parameter für das Modul `i82365` auf; vgl. die Manualpage von `i82365`. Falls `yenta_socket` verwendet wird, werden diese Optionen ignoriert, da `yenta_socket` keine Optionen kennt.

Die Zuordnung von Treibern zu PCMCIA-Karten für den Cardmanager befindet sich in den Dateien `/etc/pcmcia/config` und `/etc/pcmcia/*.conf`. Zuerst wird `config` gelesen und dann die `*.conf` in alphabetischer Reihenfolge. Der zuletzt gefundene Eintrag für eine Karte ist ausschlaggebend. Details über die Syntax dieser Dateien befinden sich in der Manualpage von `pcmcia`.

Netzwerkkarten (Ethernet, Wireless LAN und TokenRing)

Diese lassen sich wie gewöhnliche Netzwerkkarten mit YaST einrichten. Dort muss lediglich `PCMCIA` als Kartentyp ausgewählt werden. Alle weiteren Details zur Netzwerkeinrichtung befinden sich im Kapitel 21.4 auf Seite 481. Beachten Sie dort die Hinweise zu hotplugfähigen Karten.

ISDN

Auch bei ISDN-PC-Karten erfolgt die Konfiguration größtenteils wie bei sonstigen ISDN-Karten mit YaST. Es spielt keine Rolle welche der dort angebotenen PCMCIA ISDN-Karten ausgewählt wird; wichtig ist nur, dass es eine PCMCIA-Karte ist. Bei der Einrichtung der Hardware und der Provider ist darauf zu achten, dass der Betriebsmodus immer auf `hotplug`, nicht auf `onboot` steht.

So genannte ISDN-Modems gibt es auch bei PCMCIA-Karten. Dies sind Modem- oder Multifunktionskarten mit einem zusätzlichen ISDN-Connection-Kit und werden wie ein Modem behandelt.

Modem

Bei Modem-PC-Karten gibt es im Normalfall keine PCMCIA-spezifischen Einstellungen. Sobald ein Modem eingeschoben wird, steht dieses unter `/dev/modem` zur Verfügung.

Es gibt auch bei PCMCIA-Karten so genannte Softmodems. Diese werden in der Regel nicht unterstützt. Falls es Treiber gibt, müssen diese individuell ins System eingebunden werden.

SCSI und IDE

Das passende Treibermodul wird vom Cardmanager oder Hotplug geladen. Sobald also eine SCSI- oder IDE-Karte eingeschoben wird, stehen die daran angeschlossenen Geräte zur Verfügung. Die Gerätenamen werden dynamisch ermittelt. Informationen über vorhandene SCSI- bzw. IDE-Geräte sind unter `/proc/scsi/` bzw. unter `/proc/ide/` zu finden.

Externe Festplatten, CD-ROM-Laufwerke und ähnliche Geräte müssen eingeschaltet sein, bevor die PCMCIA-Karte in den Steckplatz eingeschoben wird. SCSI-Geräte müssen aktiv terminiert werden.

Achtung

Bevor eine SCSI- oder IDE-Karte entnommen wird, müssen sämtliche Partitionen der daran angeschlossenen Geräte ausgehängt werden. Wurde dies vergessen, kann erst nach einem Reboot des Systems erneut auf diese Geräte zugegriffen werden, auch wenn der Rest des Systems durchaus stabil weiterläuft.

Achtung

Sie können Linux auch vollständig auf solchen externen Platten installieren. Allerdings gestaltet sich dann der Bootvorgang etwas komplizierter. Es wird auf alle Fälle eine Bootdisk benötigt, die den Kernel und eine Initial-Ramdisk (initrd) enthält; mehr Informationen dazu finden Sie in Abschnitt 10.3 auf Seite 275.

Die `initrd` enthält ein virtuelles Dateisystem, das alle benötigten PCMCIA-Module und -Programme enthält. Die Bootdisk bzw. die Bootdisk-Images sind ebenso aufgebaut. Damit könnten Sie Ihre externe Installation immer booten. Es ist jedoch umständlich, jedes Mal die PCMCIA-Unterstützung von Hand zu laden. Fortgeschrittene Anwender können sich eine auf das jeweilige System zugeschnittene Bootdiskette selbst erstellen. Hinweise finden Sie dazu in dem englischsprachigem PCMCIA-HOWTO in Abschnitt *5.3 Booting from a PCMCIA device*.

16.1.4 Wenn's trotzdem nicht geht

Bisweilen kommt es bei der Verwendung von PCMCIA auf manchen Notebooks oder mit manchen Karten zu Problemen. Die meisten Schwierigkeiten lassen sich mit wenig Aufwand bewältigen, solange man die Sache systematisch angeht.

Achtung

Da es in SUSE LINUX sowohl externes als auch Kernel-PCMCIA nebeneinander gibt, muss beim manuellen Laden von Modulen eine Besonderheit beachtet werden. Die beiden PCMCIA-Systeme verwenden Module gleichen Namens und sind in unterschiedlichen Unterverzeichnissen unter `/lib/modules/<kernelversion>/` untergebracht. Diese Unterverzeichnisse heißen `pcmcia/` für Kernel-PCMCIA und `pcmcia-external/` für externes PCMCIA. Deshalb muss beim manuellen Laden von Modulen dieses Unterverzeichnis angegeben werden:

```
modprobe -t <verzeichnis> <modulname>
```

Achtung

Zuerst ist herauszufinden, ob das Problem mit einer Karte zusammenhängt, oder ob ein Problem des PCMCIA-Basissystems vorliegt. Deshalb sollten Sie in jedem Fall den Computer zunächst ohne eingeschobene Karten starten. Erst wenn das Basissystem einwandfrei zu funktionieren scheint, wird die Karte eingeschoben. Alle aufschlussreichen Meldungen werden in `/var/log/messages/` protokolliert. Deshalb sollte die Datei mit `tail -f /var/log/messages` während der notwendigen Tests beobachtet werden. So lässt sich der Fehler auf einen der beiden folgenden Fälle einschränken.

Das PCMCIA-Basissystem funktioniert nicht

Wenn das System beim Booten bereits bei der Meldung "PCMCIA: Starting services" stehen bleibt oder andere merkwürdige Dinge geschehen, kann das Starten von PCMCIA beim nächsten Booten durch die Eingabe von `NOPCMCIA=yes` am Bootprompt verhindert werden. Um den Fehler weiter einzugrenzen, werden nun die drei Basismodule des verwendeten PCMCIA Systems von Hand nacheinander geladen.

Um die PCMCIA-Module per Hand nachzuladen rufen Sie im Fall des *externen* PCMCIA als Benutzer `root` die Kommandos `modprobe -t <dir> pcmcia_core` und `modprobe -t pcmcia-external i82365` auf. Im Fall von *Kernel* PCMCIA rufen Sie als zweites Kommando `modprobe -t pcmcia yenta_socket` auf. In sehr seltenen Fällen rufen Sie die Kommandos `modprobe -t <dir> tcic` und `modprobe -t <dir> ds` auf. Die kritischen Module sind die beiden ersten.

Tritt der Fehler beim Laden von `pcmcia_core` auf, hilft die Manpage zu `pcmcia_core` weiter. Die darin beschriebenen Optionen können zunächst zusammen mit dem Kommando modprobe getestet werden. Als Beispiel können wir die APM-Unterstützung der PCMCIA-Module abschalten; in wenigen Fällen kann es damit Probleme geben. Dafür gibt es die Option `doapm`; mit `do_apm=0` wird das Powermanagement deaktiviert:

```
modprobe -t <dir> pcmciacore do_apm=0
```

Führt die gewählte Option zum Erfolg, wird sie in der Datei `/etc/sysconfig/pcmcia` in die Variable `PCMCIA_CORE_OPTS` geschrieben:

```
PCMCIA_CORE_OPTS="do_apm=0"
```

Vereinzelt kann das Prüfen freier IO-Bereiche Ärger machen, wenn sich dadurch andere Hardwarekomponenten gestört fühlen. Das umgeht man dann mit `probe_io=0`. Sollen mehrere Optionen verwendet werden, müssen sie durch Leerzeichen getrennt werden:

```
PCMCIA_CORE_OPTS=do_apm=0 probe_io=0
```

Wenn es beim Laden des Moduls `i82365` zu Fehlern kommt, hilft die Manualpage von `i82365`.

Ein Problem in diesem Zusammenhang ist ein Ressourcenkonflikt, ein Interrupt, IO-Port oder Speicherbereich wird doppelt belegt. Das Modul `i82365` prüft zwar diese Ressourcen, bevor sie für eine Karte zur Verfügung gestellt werden, jedoch führt manchmal genau diese Prüfung zum Problem. So führt das Prüfen des Interrupt 12 (PS/2-Geräte) bei manchen Computern zum Blockieren von Maus und/oder Tastatur. In diesem Fall hilft der Parameter `irq_list=<ListevonIRQs>`. Die Liste soll alle IRQs enthalten, die verwendet werden dürfen. Also `modprobe i82365 irq_list=5,7,9,10` oder dauerhaft in `/etc/sysconfig/pcmcia`:

```
PCMCIA_PCIC_OPTS="irq_list=5,7,9,10"
```

Weiterhin gibt es `/etc/pcmcia/config` und `/etc/pcmcia/config.opts`. Diese Dateien werden vom Cardmanager ausgewertet. Die darin gemachten Einstellungen sind erst für das Laden der Treiber-Module für die PCMCIA-Karten relevant.

In `/etc/pcmcia/config.opts` können auch IRQs, IO-Ports und Speicherbereiche ein- oder ausgeschlossen werden. Der Unterschied zur Option `irqlist` ist, dass die in der Datei `config.opts` ausgeschlossenen Ressourcen zwar nicht für eine PCMCIA-Karte verwendet, aber dennoch vom Basis-Modul `i82365` geprüft werden.

Die PCMCIA-Karte funktioniert nicht (richtig)

Hier gibt es im Wesentlichen drei Varianten: Die Karte wird nicht erkannt, der Treiber kann nicht geladen werden oder das Interface, das vom Treiber bereitgestellt wird, wurde falsch eingerichtet.

Man sollte beachten, ob die Karte vom Cardmanager oder von Hotplug behandelt wird. Nochmal zur Erinnerung: Bei externem PCMCIA regiert immer der Cardmanager, bei Kernel-PCMCIA behandelt der Cardmanager PC-Card-Karten und Hotplug behandelt CardBUS-Karten. Hier wird nur der Cardmanager besprochen.

Die Karte wird nicht erkannt Wenn die Karte nicht erkannt wird, erscheint in `/var/log/messages` die Meldung "unsupported Card in Slot x". Diese Meldung besagt lediglich, dass der Cardmanager der Karte keinen Treiber zuordnen kann. Zu dieser Zuordnung wird `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` benötigt. Diese Dateien sind sozusagen die Treiberdatenbank. Diese Treiberdatenbank lässt sich am leichtesten erweitern, wenn man vorhandene Einträge als Vorlage nimmt. Sie können mit dem Kommando `cardctl ident` herausfinden, wie die Karte sich identifiziert. Weitere Informationen dazu befinden sich im PCMCIA-HOWTO (Abschnitt 6) und in der Manualpage von `pcmcia`. Nach der Änderung von `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` muss die Treiberzuordnung neu geladen werden; dazu genügt ein `rcpcmcia reload`.

Treiber wird nicht geladen Eine Ursache hierfür besteht darin, dass in der Treiberdatenbank eine falsche Zuordnung gespeichert ist. Das kann zum Beispiel daher kommen, dass ein Hersteller in ein äußerlich unverändertes Kartenmodell einen anderen Chip einbaut. Manchmal gibt es auch alternative Treiber, die bei bestimmten Modellen besser (oder überhaupt erst) funktionieren als der voreingestellte Treiber. In diesen Fällen werden genaue Informationen über die Karte benötigt. Hier hilft auch, eine Mailingliste oder den Advanced Support Service zu fragen.

Eine weitere Ursache ist ein Ressourcenkonflikt. Bei den meisten PCMCIA-Karten ist es nicht relevant, mit welchem IRQ, IO-Port oder Speicherbereich sie betrieben werden, aber es gibt auch Ausnahmen. Dann sollte man zuerst immer nur eine Karte testen und evtl. auch andere Systemkomponenten wie zum Beispiel Soundkarte, IrDA, Modem oder Drucker vorübergehend abschalten. Die Ressourcenverteilung des Systems kann man mit `lsdev` einsehen (Es ist durchaus normal, dass mehrere PCI Geräte denselben IRQ verwenden).

Eine Lösungsmöglichkeit wäre, eine geeignete Option für das Modul `i82365` zu verwenden (siehe oben `PCMCIA_PCIC_OPTS`). Es gibt jedoch auch für manche Kartentreibermodule Optionen. Diese lassen sich mit `modinfo /lib/modules/<richtigesPCMCIA-Verzeichnis>/<treiber>.o` herausfinden (der vollständige Pfad ist hier wieder nötig, um den Treiber vom richtigen PCMCIA-System anzusprechen). Für die meisten Module gibt es auch eine Manualpage.

`rpm -ql pcmcia | grep man` listet alle im pcmcia enthaltene Manualpages auf. Zum Testen der Optionen können die Kartentreiber auch von Hand entladen werden. Hierbei ist wieder zu beachten, dass das Modul des gerade verwendeten PCMCIA-Systems zu verwenden. Siehe die Warnung weiter oben.

Wenn eine Lösung gefunden wurde, kann in `/etc/pcmcia/config.opts` die Verwendung einer bestimmten Ressource allgemein erlaubt bzw. verboten werden. Auch die Optionen für Kartentreiber finden hier Platz. Soll zum Beispiel das Modul `pcnet_cs` ausschließlich mit dem IRQ 5 betrieben werden, wird folgender Eintrag benötigt:

```
module pcnet_cs opts irq_list=5
```

Mit 10/100-MBit-Netzwerkkarten tritt manchmal das Problem auf, dass die Übertragungsart nicht automatisch richtig erkannt wird. Hier hilft das Kommando `ifport` oder `mii_tool`. Damit lässt sich die eingestellte Übertragungsart anzeigen und verändern. Um diese Kommandos automatisch ausführen zu lassen, muss das Skript `/etc/pcmcia/network` individuell angepasst werden.

Interface wird falsch konfiguriert In diesem Fall ist es empfehlenswert, die Konfiguration des Interfaces nochmal genau zu überprüfen, um seltene Konfigurationsfehler auszuschließen. Bei Netzwerkkarten kann außerdem die Dialograte der Netzwerkskripten erhöht werden, in dem man in `/etc/sysconfig/network/config` der Va-

riable `DEBUG` den Wert `yes` zuweist. Bei anderen Karten, oder wenn das noch nicht hilft, gibt es noch die Möglichkeit, in das vom Cardmanager aufgerufene Skript (siehe `/var/log/messages`) eine Zeile `set -x` einzubauen. Dadurch wird jedes einzelne Kommando des Skripts im Systemlog protokolliert. Hat man die kritische Stelle in einem Skript gefunden, können die entsprechenden Kommandos auch in einem Terminal eingegeben und getestet werden.

16.1.5 Installation via PCMCIA

In manchen Fällen wird PCMCIA bereits zum Installieren benötigt, wenn man über Netzwerk installieren möchte oder das CD-ROM via PCMCIA betrieben wird. Dazu muss man mit einer Bootdiskette starten. Des Weiteren wird eine der Moduldisketten benötigt.

Nach dem Booten von Diskette (oder auch nach der Auswahl 'manuelle Installation' beim Booten von CD) wird das Programm linuxrc gestartet. Dort muss unter dem Menüpunkt 'Kernel-Module (Hardware-Treiber)' der Punkt 'Lade PCMCIA Module' ausgewählt werden. Zuerst erscheinen zwei Eingabefelder, in denen man Optionen für die Module `pcmcia_core` und `i82365` eingeben kann. Im Normalfall bleiben diese Felder jedoch leer. Die Manualpages für `pcmcia_core` und `i82365` befinden sich als Textdateien auf der ersten CD im Verzeichnis `docu/`.

Bei SUSE LINUX wird mit dem externen PCMCIA-System installiert. Während der Installation werden Systemmeldungen auf verschiedenen virtuellen Konsolen ausgegeben, auf die man mit (Alt) + (Funktionstaste) umschalten kann.

Später, wenn bereits eine grafische Oberfläche aktiv ist, muss man (Strg) + (Alt) + (Funktionstaste) verwenden.

Es gibt auch schon während der Installation Terminals, auf denen Kommandos ausgeführt werden können. Solange linuxrc läuft, ist das die Konsole 9 (eine sehr spartanisch ausgestattete Shell); sobald das Installationssystem geladen ist (YaST wurde gestartet) gibt es auf Konsole 2 eine bash und viele gängige Systemtools.

Wenn während der Installation ein falsches Treibermodul für eine PCMCIA Karte geladen wird, muss die Bootdiskette von Hand angepasst werden. Dazu benötigt man jedoch fortgeschrittene Linuxkenntnisse. Wenn der erste Teil der Installation abgeschlossen ist, wird das System teilweise oder ganz neu gestartet. Dabei kann in seltenen Fällen beim Starten von PCMCIA das System stehen bleiben. Zu diesem Zeitpunkt ist die Installation aber schon weit genug fortgeschritten, sodass mit der Boot-Option

`NOPCMCIA=yes` Linux ohne PCMCIA gestartet werden kann, zumindest im Textmodus. Hier hilft der Abschnitt 16.1.4 auf Seite 366 weiter. Evtl. kann man schon vor Abschluss des ersten Teils der Installation auf Konsole 2 einige Einstellungen am System verändern, so dass der Neustart erfolgreich verläuft.

16.1.6 Weitere Hilfsprogramme

Das Programm cardctl wurde schon mehrfach erwähnt. Diese Applikation ist das wesentliche Werkzeug, um Informationen von PCMCIA zu erhalten bzw. bestimmte Aktionen auszuführen. In der Datei `cardctl` finden Sie Details; oder Sie geben `cardctl` ein und erhalten eine Liste der gültigen Kommandos.

Zu diesem Programm gibt es auch ein grafisches Frontend cardinfo, mit dem die wichtigsten Dinge kontrollierbar sind. Dazu muss jedoch das Paket `pcmcia-cardinfo` installiert sein.

Weitere Helfer aus dem `pcmcia` Paket sind `ifport`, `ifuser`, `probe` und `rcpcmcia`. Diese werden aber nicht immer benötigt. Um genau zu erfahren, was alles im Paket `pcmcia` steckt, verwendet man den Befehl `rpm -ql pcmcia`.

16.1.7 Kernel oder PCMCIA Paket aktualisieren

Wenn Sie den Kernel aktualisieren möchten, sollten Sie die von SUSE bereitgestellten Kernelpakete verwenden. Ist es notwendig, einen eigenen Kernel zu kompilieren, dann müssen auch die PCMCIA-Module neu kompiliert werden. Wichtig ist, dass während der Neuübersetzung bereits der richtige Kernel läuft, da aus diesem einige Informationen extrahiert werden. Das `pcmcia` Paket sollte bereits installiert, aber nicht gestartet sein; im Zweifelsfall sollte Sie noch `rcpcmcia stop` ausführen. Dann installiert man das PCMCIA-Quellpaket mit und gibt anschließend ein:

```
rpm -ba /usr/src/packages/SPECS/pcmcia.spec
```

Danach liegen unter `/usr/src/packages/RPMS/` neue Pakete. Das Paket `pcmcia-modules` enthält die PCMCIA-Module für externes PCMCIA. Dieses Paket muss mit `rpm --force` installiert werden, da die Moduldateien offiziell zum Kernel-Paket gehören.

16.1.8 Weiterführende Informationen

Wer an Erfahrungen mit bestimmten Notebooks interessiert ist, sollte auf alle Fälle die Linux Laptop Homepage unter `http://linux-laptop.net` besuchen. Eine weitere gute Informationsquelle ist die TuxMobil-Homepage unter `http://tuxmobil.org/`. Dort findet man neben viele interessanten Informationen auch ein Laptop-Howto und ein IrDA-Howto. Außerdem gibt es in der Supportdatenbank mehrere Artikel zum mobilen Arbeiten unter SUSE LINUX. Suchen Sie unter `http://portal.suse.de/sdb/de/index.html` unter dem Stichwort *Laptop*.

16.2 SCPM – System Configuration Profile Management

Es gibt Situationen, in denen eine veränderte Konfiguration des Computersystems benötigt wird. Am häufigsten trifft dies auf mobile Computer zu, die an verschiedenen Standorten betrieben werden. Es kann aber auch sein, dass man auf einem Desktopsystem zeitweilig andere Hardwarekomponenten verwendet. In jedem Fall sollte eine Rückkehr zum ursprünglichen System einfach sein. Noch besser ist es, wenn diese Umkonfiguration auch noch einfach reproduzierbar ist.

Eine Lösung für dieses Problem gab es bisher nur für PCMCIA-Hardware. Dort konnte man verschiedene Konfigurationen in bestimmten Schemata ablegen. Ausgehend davon haben wir SCPM (engl. *System Configuration Profile Management*) entwickelt, das die Beschränkung auf PCMCIA aufhebt. Mit SCPM lässt sich ein frei wählbarer Teil der Systemkonfiguration festlegen, von dem verschiedene Zustände in eigenen Konfigurationsprofilen festgehalten werden können. Etwas freier ausgedrückt ist das, als ob man Schnappschüsse von seiner Systemkonfiguration macht, die man jederzeit wiederherstellen kann.

Das Hauptanwendungsgebiet wird vermutlich bei der Netzwerkkonfiguration von Laptops liegen. Aber unterschiedliche Netzwerkeinstellungen beeinflussen meist auch noch andere Elemente, zum Beispiel die Einstellungen für e-Mail oder Proxies. Hierzu kommen unterschiedliche Drucker zu Hause und in der Firma oder die gesonderte XFree-Konfiguration für den Beamer bei Vorträgen, besonders sparsame Stromverbrauchseinstellungen für unterwegs oder eine andere Zeitzone in der Auslandsniederlassung.

Mit vermehrten Einsatz dieses Werkzeugs bilden sich immer wieder neue Anforderungen heraus. Wenn Sie selbst Anregungen und Kritik zu SCPM haben, dann nehmen Sie mit uns Kontakt auf. Wir sind sehr an Rückmeldungen interessiert. Wir haben SCPM auf ein flexibles Grundgerüst gestellt, sodass zum Beispiel auch ein serverbasiertes Profil Management möglich ist. Bitte teilen Sie uns Ihre Wünsche, Anregungen und Fehlerbeschreibungen über unser Webfrontend `http://www.suse.de/feedback` mit.

16.2.1 Grundbegriffe und Grundlagen

Vorab sollen einige Grundbegriffe festgelegt werden, die auch in der restlichen Dokumentation zu SCPM und im YaST-Modul so verwendet werden.

- Unter *Systemkonfiguration* verstehen wir die gesamte Konfiguration des Computers. Alle grundlegenden Einstellungen, wie die zum Beispiel Verwendung von Festplattenpartitionen oder Netzwerkeinstellungen, Zeitzonenauswahl oder Tastatureinstellungen.
- Ein *Profil* oder auch *Konfigurationsprofil* ist ein Zustand der Systemkonfiguration, der festgehalten wurde und der bei Bedarf einfach wiederhergestellt werden kann.
- Als *aktives Profil* wird immer das Profil bezeichnet, in das zuletzt geschaltet wurde. Das heißt nicht, dass die aktuelle Systemkonfiguration exakt diesem Profil entspricht, denn die Konfiguration kann jederzeit individuell verändert werden.
- *Resource* im Sinne von SCPM sind alle Elemente, die zur Systemkonfiguration beitragen. Das kann eine Datei oder ein Softlink einschließlich ihrer Metadaten, wie Benutzer, Rechte oder Zugriffszeit sein. Das kann aber auch ein Systemdienst sein, der einmal läuft und in einem anderen Profil ausgeschaltet ist.
- Die Ressourcen sind in sogenannten *Resource Groups* organisiert. Diese Gruppen enthalten jeweils Ressourcen, die logisch zusammenpassen. Für die meisten Gruppen bedeutet das, dass sie einen Dienst und die dazugehörigen Konfigurationsdateien enthalten. Dieser Mechanismus erlaubt das einfache Zusammenstellen der Ressourcen, die von SCPM behandelt werden, ohne wissen zu müssen, welche Konfigurationsdateien für welche Dienste notwendig wären. SCPM beinhaltet bereits eine Vorauswahl an aktivierten Resource Groups, die für die meisten Benutzer ausreichend sein sollte.

16.2.2 Der YaST Profil-Manager und weiterführende Dokumentation

Als grafisches Frontend zu SCPM (Paket `scpm`) gibt es ein YaST-Modul (Paket `yast2-profile-manager`) als Alternative zu dem Kommandozeilen-Frontend. Da die Funktionalität beider Frontends im Wesentlichen dieselbe ist und die Kenntnis des Kommandozeilen-Frontends für viele Zwecke interessant ist, wird hier nur das letztere beschrieben. Die Bedienung des SCPM YaST-Moduls ist danach zusammen mit den dort angebotenen Hilfetexten sehr leicht. Die wenigen Besonderheiten des YaST-Moduls werden an passender Stelle erwähnt.

Die aktuellste Dokumentation ist in den Infoseiten zu SCPM zu finden. Diese kann mit Werkzeugen wie Konqueror oder Emacs eingesehen werden (`konqueror info:scpm`). In der Konsole verwendet man `info` oder `pinfo`. Technische Dokumentation für Benutzer, die selbst Hand an SCPM legen möchten, gibt es unter `/usr/share/doc/packages/scpm/`. Der Aufruf von `scpm` ohne weitere Argumente gibt eine Kommandoübersicht aus.

16.2.3 SCPM einrichten

Bevor mit SCPM gearbeitet werden kann, muss es erst einmal eingeschaltet werden. Standardmäßig behandelt SCPM Netzwerk- und Druckereinstellungen, sowie die XFree86 Konfiguration und einige Netzwerkdienste. Falls Sie darüber hinaus Dienste oder Konfigurationsdateien verwaltet haben möchten, sollten Sie noch die entsprechenden Resource Groups aktivieren. Die bereits definierten Resource Groups können Sie mit dem Befehl `scpm list_groups` anzeigen lassen, wenn Sie nur die bereits aktiven Gruppen sehen möchten, geben Sie `scpm list_groups -a` ein. Die Kommandozeilenbefehle müssen als Benutzer `root` ausgeführt werden. Aktivieren bzw. Deaktivieren können Sie die Gruppen mit `scpm activate_group NAME` bzw. `scpm deactivate_group NAME`, wobei `NAME` durch den enstprechenden Gruppennamen zu ersetzen ist. Sie können die Resource Groups auch bequem mit Hilfe des YaST Profil-Managers konfigurieren.

Mit dem Aufruf von `scpm enable` wird SCPM eingeschaltet. Beim ersten Einschalten wird SCPM initialisiert, was einige Sekunden in Anspruch nimmt. SCPM kann mit `scpm disable` jederzeit ausgeschaltet werden, um unbeabsichtigte Profilumschaltungen zu vermeiden. Beim anschließenden Wiedereinschalten wird der Betrieb einfach fortgesetzt.

16.2.4 Profile anlegen und verwalten

Nachdem SCPM eingeschaltet wurde, gibt es bereits ein Profil namens `default`. Eine Liste aller verfügbaren Profile gibt das Kommando `scpm list` aus. Dieses bisher einzige Profil ist zwangsläufig auch das aktive Profil. Das erfährt man mit `scpm active`. Das Profil `default` ist als Grundkonfiguration gedacht, von der die anderen Profile abgeleitet werden. Deshalb sollten zuerst alle Einstellungen, die in allen Profilen einheitlich sein sollen, vorgenommen werden. Mit `scpm reload` werden diese Änderungen dann im aktiven Profil gespeichert. Das Profil `default` kann dennoch beliebig verwendet, umbenannt oder gelöscht werden.

Es gibt zwei Möglichkeiten, ein neues Profil hinzuzufügen. Wenn das neue Profil (hier mit Namen `work`) zum Beispiel auf dem Profil `default` basieren soll, geschieht dies mit `scpm copy default work`. Danach kann man mit `scpm switch work` in das neue Profil umschalten und es dann konfigurieren. Manchmal hat man aber auch die Systemkonfiguration schon für bestimmte Zwecke verändert und möchte diese danach in einem neuen Profil festhalten. Das erledigt der Aufruf von `scpm add work`. Jetzt ist die aktuelle Systemkonfiguration im Profil `work` gesichert und das neue Profil als aktiv markiert; das heisst ein `scpm reload` sichert Änderungen jetzt im Profil `work`.

Selbstverständlich können Profile auch umbenannt oder gelöscht werden. Dafür gibt es die Kommandos `scpm rename x y` und `scpm delete x`. Um zum Beispiel `work` nach `arbeit` umzubenennen und es hinterher zu löschen, gibt man `scpm rename work arbeit` und dann `scpm delete arbeit` ein. Nur das aktive Profil kann nicht gelöscht werden.

Hinweis zum YaST-Modul: Hier gibt es nur den Knopf 'Hinzufügen'. Es erscheint dann aber die Frage, ob man ein existierendes Profil kopieren oder die gegenwärtige Systemkonfiguration sichern möchte. Zum Umbenennen verwendet man dort den Knopf 'Ändern'.

16.2.5 Zwischen Konfigurationsprofilen umschalten

Das Umschalten zu einem anderen Profil (hier `work`) wird mit dem Kommando `scpm switch work` ausgelöst. Es ist zulässig, zum gerade aktiven Profil umzuschalten um geänderte Einstellungen an der Systemkonfiguration zu sichern. Alternativ kann dafür aber auch das Kommando `scpm reload` verwendet werden.

Um den Umschaltvorgang und die dabei eventuell auftretenden Fragen besser zu verstehen, soll dieser hier näher erläutert werden. Zuerst prüft

SCPM, welche Ressourcen des aktiven Profils seit dem letzten Umschalten verändert wurden. Aus der Liste der veränderten Ressourcen wird die Liste der geänderten Resource Groups erzeugt. Für jede dieser Gruppen wird anschließend nachgefragt, ob die Änderungen in das noch aktive Profil übernommen werden sollen. Falls Sie – wie es bei früheren Versionen von SCPM der Fall war – lieber die einzelnen Ressourcen angezeigt bekommen möchten, dann rufen Sie den Switch-Befehl mit dem Parameter `-r` auf, etwa so: `scpm switch -r work`.

Danach vergleicht SCPM die aktuelle Systemkonfiguration mit dem neuen Profil, in das umgeschaltet werden soll. Dabei wird ermittelt, welche Systemdienste aufgrund von Konfigurationsänderungen oder wegen gegenseitiger Abhängigkeiten angehalten bzw. (wieder) gestartet werden müssen. Das kann man sich wie einen teilweisen Systemreboot vorstellen, nur dass eben nur ein kleiner Teil des Systems betroffen ist und der Rest unverändert weiterarbeitet.

Erst jetzt laufen folgende Aktionen ab:

1. Die Systemdienste werden angehalten.
2. Alle veränderten Ressourcen (zum Beispiel Konfigurationsdateien) werden geschrieben.
3. Die Systemdienste werden (wieder) gestartet.

16.2.6 Erweiterte Profileinstellungen

Sie können für jedes Profil eine Beschreibung eingeben, die dann bei `scpm list` mit ausgegeben wird. Eingeben kann man diese Beschreibung für das gerade aktive Profil mit dem Kommando `scpm set description "text"`. Für nicht aktive Profile muss noch das Profil angegeben werden, also `scpm set description "text" work`

Manchmal kommt es vor, dass beim Umschalten in ein anderes Profil zusätzliche Aktionen ausgeführt werden sollen, die in SCPM (noch) nicht vorgesehen sind. Dafür können für jedes Profil vier ausführbare Programme oder Skripte eingehängt werden, die zu verschiedenen Zeitpunkten während das Umschaltens ausgeführt werden. Diese Zeitpunkte sind:

prestop vor dem Anhalten von Diensten beim Verlassen des Profils

poststop nach dem Anhalten von Diensten beim Verlassen des Profils

prestart vor dem Starten von Diensten beim Aktivieren des Profils

poststart nach dem Starten von Diensten beim Aktivieren des Profils

Das Umschalten von Profil `work` zu Profil `home` läuft dann folgendermaßen ab:

1. Prestop-Aktion des Profils `work` wird ausgeführt.
2. Anhalten von Diensten
3. Poststop-Aktion des Profils `work` wird ausgeführt.
4. Verändern der Systemkonfiguration
5. Prestart-Aktion des Profils `home` wird ausgeführt.
6. Starten von Diensten
7. Poststart-Aktion des Profils `home` wird ausgeführt.

Diese Aktionen werden auch mit dem `set` Kommando eingehängt, nämlich mit `scpm set prestop <dateiname>`, `scpm set poststop <dateiname>`, `scpm set prestart <dateiname>` oder `scpm set poststart <dateiname>`. Es muss sich dabei um ein ausführbares Programm handeln, das heisst Skripte müssen den richtigen Interpreter beinhalten und zumindest für den Superuser (`root`) ausführbar sein.

Achtung

Da diese Skripte oder Programme mit den Rechten des Superusers ausgeführt werden sollten sie nicht von beliebigen Anwendern änderbar sein. Da in Skripten durchaus vertrauliche Informationen enthalten sein können, ist es sogar angeraten, dass diese nur vom Superuser lesbar sind. Am besten versieht man diese Programme mit den Rechten `-rwx---- root root`.

```
chmod 700 <dateiname>
chown root.root <dateiname>
```

Achtung

Alle Zusatzeinstellungen, die mit `set` eingegeben wurden, lassen sich mit `get` abfragen. Zum Beispiel liefert `scpm get poststart` den Namen des

Poststartprogramms oder einfach keine Information, wenn nichts eingehängt wurde. Gelöscht werden solche Einstellungen durch Überschreiben mit `""`; das heisst der Aufruf von `scpm set prestop ""` hängt das Poststop-Programm wieder aus.

Genau wie beim Anlegen der Beschreibung können alle `set` und `get` Kommandos für ein beliebiges Profil angewandt werden. Dazu wird zuletzt noch der Name des Profils angegeben. Zum Beispiel `scpm get prestop <dateiname> work` oder `scpm get prestop work`.

16.2.7 Profilauswahl beim Booten

Es ist möglich, schon vor dem Booten ein Profil auszuwählen. Dazu muss lediglich der Bootparameter `PROFILE=<Name des Profils>` am Bootprompt eingegeben werden.

In der Bootloaderkonfiguration (`/boot/grub/menu.lst`) wird für die Option `title` ebenfalls der Name des Profils verwendet. Standardmäßig wird GRUB als Bootloader verwendet. Eine ausführlichere Beschreibung finden Sie Abschnitt 8.4 auf Seite 227; alternativ geben Sie `info grub` ein. Die Konfiguration von GRUB sieht dann zum Beispiel wie folgt aus:

Beispiel 16.1: *Die Datei /boot/grub/menu.lst*

```
gfxmenu (hd0,5)/boot/message
color white/green black/light-gray
default 0
timeout 8

title work
   kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=work
   initrd (hd0,5)/boot/initrd

title home
   kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=home
   initrd (hd0,5)/boot/initrd

title road
   kernel (hd0,5)/boot/vmlinuz root=/dev/hda6 PROFILE=road
   initrd (hd0,5)/boot/initrd
```

Für Systeme, die noch den Bootloader LILO verwenden, kann das Beispiel 16.2 auf der nächsten Seite benutzt werden.

Beispiel 16.2: *Die Datei /etc/lilo.conf*

```
boot    = /dev/hda
change-rules
reset
read-only
menu-scheme = Wg:kw:Wg:Wg
prompt
timeout = 80
message = /boot/message

  image  = /boot/vmlinuz
  label  = home
  root   = /dev/hda6
  initrd = /boot/initrd
  append = "vga=0x317 hde=ide-scsi PROFILE=home"

  image  = /boot/vmlinuz
  label  = work
  root   = /dev/hda6
  initrd = /boot/initrd
  append = "vga=0x317 hde=ide-scsi PROFILE=work"

  image  = /boot/vmlinuz
  label  = road
  root   = /dev/hda6
  initrd = /boot/initrd
  append = "vga=0x317 hde=ide-scsi PROFILE=road"
```

Jetzt kann beim Booten sehr einfach das gewünschte Profil ausgewählt werden.

16.2.8 Probleme und deren Lösung

Normalerweise sollte der Betrieb von SCPM reibungslos funktionieren. Es gibt aber einige Fallstricke, die hier beschrieben werden.

SCPM ist zum jetzigen Zeitpunkt noch nicht in der Lage, ein Systemupdate zu verwalten. Die Schwierigkeit liegt darin, dass bei einem Systemupdate die Daten, die in den Profilen gespeichert sind, von den verschiedenen Updatemechanismen nicht aktualisiert werden können. SCPM erkennt daher, falls ein Systemupdate gemacht wurde, und verweigert seinen Dienst. Sie

sollten in dieser Sitation eine Fehlermeldung von SCPM erhalten, die "Ihre Betriebsysteminstallation hat sich geändert oder ist unbekannt" enthält. In diesem Fall reinitialisieren Sie SCPM einfach mit `scpm -f enbale` neu. Die Profile sind dann allerdings verloren, d.h. Sie müssen sie neu einrichten.

Unter Umständen kann es auch vorkommen, dass SCPM während eines Switch-Vorgangs unvermittelt abbricht. Das kann entweder aufgrund äußerer Einwirkung eintreten – zum Beispiel Abbruch durch den Benutzer, Leerlaufen des Notebookakkus o.ä. – oder es kann ein Fehler in SCPM selbst sein. Dann werden Sie beim nächsten SCPM Aufruf die Meldung erhalten, dass SCPM gesperrt ist. Dies dient zum Schutz Ihres Systems, da die Daten, die SCPM in seiner Datenbank gespeichert hat, eventuell nicht zu dem Zustand Ihres System passen. Löschen Sie in diesem Fall die Lock-Datei mit `rm /var/lib/scpm/#LOCK` und stellen Sie mit `scpm -s reload` wieder einen konsistenten Status her. Anschließend können Sie wie gewohnt weiterarbeiten.

Noch ein Hinweis: Wenn Sie bei bereits initialisiertem SCPM die Resource Group Konfiguration ändern möchten, ist das prinzipiell kein Problem. Sie müssen nur darauf achten, daß Sie, nachdem Sie mit dem Hinzufügen oder Entfernen von Gruppen fertig sind, `scpm rebuild` aufrufen. Dies fügt neue Ressourcen zu allen Profilen hinzu und löscht die entfernten. Letztere sind dann allerdings endgültig gelöscht, wenn Sie diese in den verschiedenen Profilen verschieden konfiguriert haben, verlieren Sie diese Konfigurationsdaten – bis auf die aktuelle Version in Ihrem System natürlich, diese wird von SCPM nicht angefasst. Falls Sie die Konfiguration mit YaST verändern, ist kein Rebuild-Aufruf nötig, dies erledigt dann YaST für Sie.

16.3 IrDA – Infrared Data Association

IrDA (engl. *Infrared Data Association*) ist ein Industriestandard für drahtlose Kommunikation über Infrarotlicht. Viele heute ausgelieferte Laptops sind mit einem IrDA-kompatiblen Sender/Empfänger ausgestattet, der die Kommunikation mit anderen Geräten, wie Druckern, Modems, LAN oder anderen Laptops ermöglicht. Die Übertragungsrate reicht von 2400 bps bis hin zu 4 Mbps.

Es gibt zwei Betriebsmodi für IrDA. Im Standardmodus SIR wird der Infrarotport über eine serielle Schnittstelle angesprochen. Dieser Modus funktioniert auf fast allen Geräten und genügt für viele Anforderungen. Der

schnellere Modus FIR benötigt einen speziellen Treiber für den IrDA-Chip. Es gibt aber nicht für alle Chips solche Treiber. Außerdem muss der gewünschte Modus im BIOS-Setup des Computers eingestellt werden. Dort erfährt man meist auch, welche serielle Schnittstelle für den SIR-Modus verwendet wird.

Informationen zu IrDA finden Sie im IrDA-Howto von Werner Heuser unter `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html` und auf der Homepage des Linux IrDA Projekts: `http://irda.sourceforge.net/`.

16.3.1 Software

Die notwendigen Kernelmodule sind im Kernelpaket enthalten. Das Paket `irda` stellt die nötigen Hilfsprogramme zur Unterstützung der Infrarotschnittstelle bereit. Nach der Installation des Paketes findet man die Dokumentation unter `/usr/share/doc/packages/irda/README`.

16.3.2 Konfiguration

Der IrDA Systemdienst wird nicht automatisch beim Booten gestartet. Verwenden Sie das YaST Runlevel-Modul um die Einstellungen zu den Systemdiensten zu verändern. Alternativ kann auch das Programm `chkconfig` verwendet werden. Leider benötigt IrDA merklich mehr (Batterie-)Strom, da alle paar Sekunden ein Discovery-Paket verschickt wird, um andere Peripheriegeräte automatisch zu erkennen. Deshalb sollte man, wenn man auf Batteriestrom angewiesen ist, IrDA am besten nur bei Bedarf starten. Mit dem Kommando `rcirda start` können Sie die Schnittstelle jederzeit manuell aktivieren bzw. deaktivieren (mit dem Parameter `stop`). Beim Aktivieren der Schnittstelle werden die notwendigen Kernel-Module automatisch geladen.

In der Datei `/etc/sysconfig/irda` gibt es nur eine Variable `IRDA_PORT`. Dort können Sie einstellen, welche Schnittstelle im SIR-Modus verwendet wird; dies wird über das Skript `/etc/irda/drivers` beim Start der Infrarotunterstützung eingestellt.

16.3.3 Verwendung

Will man nun über Infrarot drucken, kann man dazu über die Gerätedatei `/dev/irlpt0` die Daten schicken. Die Gerätedatei `/dev/irlpt0` verhält

sich wie die normale drahtgebundene Schnittstelle `/dev/lp0`, nur dass die Druckdaten drahtlos über infrarotes Licht verschickt werden.

Einen Drucker, der über die Infrarotschnittstelle betrieben wird, können Sie wie einen Drucker am Parallelport oder an der seriellen Schnittstelle einrichten. Beachten Sie bitte beim Drucken, dass sich der Drucker in Sichtweite der Infrarotschnittstelle des Computers befindet und dass die Infrarotunterstützung gestartet wird.

Will man über die Infrarotschnittstelle mit anderen Rechnern, mit Handys oder ähnlichen Geräten kommunizieren, so kann man dies über die Gerätedatei `/dev/ircomm0` erledigen. Mit dem Siemens S25 Handy beispielsweise kann man sich über das Programm wvdial mittels Infrarot drahtlos ins Internet einwählen. Auch ein Datenabgleich mit dem Palm Pilot ist so möglich, dazu muss im entsprechenden Programm als Gerät einfach `/dev/ircomm0` eingegeben werden.

Beachten Sie bitte auch, dass Sie ohne weiteres nur Geräte ansprechen können, die die Protokolle Printer oder IrCOMM unterstützen. Mit speziellen Programmen (irobexpalm3, irobexreceive, bitte beachten Sie hierzu die Beschreibung im IR-HOWTO) können Sie auch Geräte ansprechen, die das IROBEX-Protokoll verwenden (3Com Palm Pilot). Die vom Gerät unterstützten Protokolle werden bei der Ausgabe von irdadump nach dem Gerätenamen in eckigen Klammern angeben. Die Unterstützung des IrLAN-Protokolls ist „work in progress“ – es ist leider zur Zeit noch nicht stabil, wird aber sicher in naher Zukunft auch unter Linux zur Verfügung stehen.

16.3.4 Troubleshooting

Falls Geräte am Infrarotport nicht reagieren, können Sie als Benutzer `root` mit dem Kommando `irdadump` überprüfen, ob das andere Gerät vom Computer erkannt wird.

Bei einem Canon BJC-80 Drucker in Sichtweite des Computers erscheint dann eine Ausgabe ähnlich der folgenden in regelmäßiger Wiederholung (vgl. Ausgabe 16.3.

Beispiel 16.3: *Ausgabe von irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
```

```
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* erde
                        hint=0500 [ PnP Computer ] (21)
```

Sollte überhaupt keine Ausgabe erfolgen oder das andere Gerät sich nicht zurückmelden, so überprüfen Sie bitte die Konfiguration der Schnittstelle. Verwenden Sie überhaupt die richtige Schnittstelle? Manchmal ist die Infrarotschnittstelle auch unter `/dev/ttyS2` oder `/dev/ttyS3` zu finden oder ein anderer Interrupt als Interrupt 3 wird verwendet. Diese Einstellungen können Sie aber bei fast jedem Laptop im BIOS-Setup konfigurieren.

Mit einer einfachen Video-Kamera können Sie auch überprüfen, ob die Infrarot-LED überhaupt aufleuchtet – im Gegensatz zum menschlichen Auge können die meisten Videokameras Infrarotlicht sehen.

16.4 Bluetooth – Geräte drahtlos verbinden

Bei Bluetooth handelt es sich um eine Funktechnologie, die verschiedenene Geräte miteinander verbindet. Bluetooth unterscheidet sich dabei in einigen wesentlichen Punkten von IrDA: Zum einen müssen die einzelnen Geräte sich nicht direkt „sehen“, zum anderen können mehrere Geräte zusammen ganze Netzwerke aufbauen. Allerdings sind nur Datenraten bis maximal 720 Kbps erreichbar (in der aktuellen Version 1.1). Theoretisch kann man mittels Bluetooth auch durch Wände hindurch „funken“. In der Praxis hängt dies aber sehr stark von den Wänden und der Geräteklasse ab. Letztere bestimmt die maximale Sendereichweite, die in drei Klassen von 10 bis 100 Metern reicht.

16.4.1 Profile

Dienste werden bei Bluetooth mittels sogenannter Profile definiert. Im Bluetooth-Standard sind z.B. Profile für den Dateitransfer („File Transfer“-Profile), Drucken („Basic Printing“-Profil) und Netzwerkverbindungen („Personal Area Network“-Profil) festgelegt.

Damit ein Gerät den Dienst eines anderen benutzen kann, müssen beide das gleiche Profil verstehen — eine Information, die manchmal leider weder der Verpackung noch dem Handbuch des Gerätes entnehmbar ist. Erschwerend kommt hinzu, dass sich zwar manche Hersteller streng an die Definitionen der einzelnen Profile halten, andere dagegen weniger. In der Regel klappt die Verständigung zwischen den Geräten aber.

16.4.2 Software

Um Bluetooth verwenden zu können braucht man einen Bluetooth-Adapter (entweder eingebaut im Gerät oder als externes Dongle), Treiber und einen sogenannten „Bluetooth Protocol Stack“.

Im Linuxkernel befindet sich bereits die Grundausstattung an Treibern für den Gebrauch von Bluetooth. Als „Protocol Stack“ kommt das Bluez-System zur Anwendung. Zusätzlich sollten noch alle mit Bluetooth in Verbindung stehenden Pakete (`bluez-libs`, `bluez-bluefw`, `bluez-pan`, `bluez-sdp` und `bluez-utils`) installiert werden, da diese einige benötigte Dienste und Dienstprogramme bereitstellen. Auf einige davon wird später noch eingegangen.

16.4.3 Konfiguration

Die nachstehend beschriebenen Konfigurationsdateien können nur als User `root` verändert werden. Eine grafische Benutzeroberfläche um die entsprechenden Parameter einzustellen, gibt es im Moment leider nicht. Die Dateien müssen also mit einem Textverarbeitungsprogramm verändert werden.

Einen ersten Schutz vor ungewollten Verbindungen bietet die Absicherung durch eine PIN-Nummer. Mobiltelefone fragen den PIN normalerweise beim ersten Kontakt (bzw. dem Einrichten eines Gerätekontaktes auf dem Telefon) ab. Damit sich zwei Geräte miteinander unterhalten können, müssen beide sich mit dem selben PIN identifizieren. Dieser befindet sich auf dem Rechner in der Datei `/etc/bluetooth/pin`. Momentan gibt es unter Linux nur einen PIN, unabhängig von der Anzahl der installierten Bluetoothgeräte. Das Ansprechen von mehreren Geräte mit unterschiedlichen PINs wird zur Zeit leider nicht unterstützt, hier müssen entweder alle Geräte auf die gleiche PIN-Nummer gesetzt werden, oder die PIN-Authentifizierung ganz deaktiviert werden.

Hinweis

Sicherheit von Bluetooth-Verbindungen

Trotz des PINs sollte man davon ausgehen, dass eine Übertragung zwischen zwei Geräten nicht abhörsicher ist!

Hinweis

Das Aktivieren geschieht in der Konfigurationsdatei `/etc/bluetooth/hcid.conf`. Hier kann man verschiedene Einstellungen wie Gerätenamen und Sicherheitsmodus ändern. Im Wesentlichen sollten die Einstellungen ausreichend sein, lediglich zwei sollen hier kurz erwähnt werden. Die Datei enthält Kommentare, die die Optionen bei den verschiedenen Einstellungen beschreiben.

Eine der wichtigsten Einstellungen ist `security auto;`. Mit dieser wird die beschriebene Notwendigkeit eines PINs zur Identifikation aktiviert, wobei durch das `auto` im Problemfall auf `keine PIN verwenden` geschaltet wird. Ob Sie diese Einstellung auf `none` setzen, so dass nie eine PIN-Nummer verwendet wird, oder auf `user` (immer verwenden) setzen, bleibt Ihnen und Ihrem Bedarf an Sicherheit überlassen.

Interessant ist der Abschnitt, der mit `device {` eingeleitet wird. Hier kann man festlegen, unter welchem Namen der Rechner bei den Gegenstellen angezeigt wird. Die Geräteklasse (`Laptop`, `Server`, etc.) wird hier ebenso definiert wie Authentifizierung und Verschlüsselung.

16.4.4 Systemkomponenten und nützliche Hilfsmittel

Erst durch das Zusammenspiel verschiedener Dienste wird Bluetooth überhaupt benutzbar. Zwei im Hintergrund laufende Daemonen werden minimal benötigt: Zum einen der hcid (*Host Controller Interface*). Dieser dient als Schnittstelle zum Bluetoothgerät und steuert dieses. Zum anderen braucht man den sdpd (*Service Discovery Protocol*). Über den sdpd kann ein Gerät herausbekommen, welche Dienste der Rechner zur Verfügung stellt. Sowohl hcid als auch sdpd können — falls nicht bereits automatisch beim Systemstart geschehen — mit dem Kommando `rcbluetooth start` in Betrieb genommen werden. Es ist dazu allerdings nötig `root` zu sein.

Hinweis

Alle erwähnten Programme verfügen über weitere Funktionalitäten, die sich mittels `man <programmname>` in Erfahrung bringen lassen.

Hinweis

Im Folgenden wird kurz auf die wichtigsten Werkzeuge eingegangen, die für das Arbeiten mit Bluetooth nötig sind. Konqueror — (KDE-Desktop) listet Ihnen mit dem URL `sdp://` lokale (d.h. physikalisch mit dem Rechner verbundene) und entfernte (d.h. nur mittels Funk erreichbaren) Bluetooth-Geräte.

Einige Kommandos lassen sich leider nur als `root` ausführen. Hierzu gehört z.B. `l2ping <Geräteadresse>`, mit dem die Verbindung zu einem entfernten Gerät getestet werden kann.

hcitool

Mittels des hcitool kann einfach festgestellt werden, ob lokale und/oder entfernte Geräte gefunden wurden. Der Kommandoaufruf `hcitool dev` sollte das eigene Gerät anzeigen. Die Ausgabe erzeugt für jedes gefundene lokale Gerät eine Zeile in der Form `<interfacename> <Geräteadresse>`.

Mit `hcitool name <Geräteadresse>` kann der Gerätename eines entfernten Gerätes ermittelt werden. Handelt es sich dabei z.B. um einen weiteren Rechner, so würde die ausgegebene Klasse und der Gerätename der Information aus dessen `/etc/bluetooth/hcid.conf` Datei entsprechen. Lokale Geräteadressen erzeugen eine Fehlerausgabe.

hciconfig

Weitere Informationen über das lokale Gerät erhält man mittels `/sbin/hciconfig`. Entfernte Geräte (die nicht physikalisch mit dem Rechner verbunden sind) werden mit `hcitool inq` gesucht. Hier werden drei Werte pro gefundenem Gerät ausgegeben: Die Geräteadresse, eine Uhrendifferenz und die Geräteklasse. Wichtig ist die Geräteadresse. Diese wird bei anderen Kommandos benutzt um das Zielgerät zu identifizieren. Die Uhrendifferenz ist im Prinzip nur aus technischer Sicht interessant. In der Klasse wird sowohl Gerätetyp als auch Servicetyp als Hexadezimalwert kodiert.

sdptool

Die Information, welcher Dienst von einem bestimmten Gerät zur Verfügung gestellt wird, erhält man durch das Programm sdptool. `sdptool browse <Geräteadresse>` liefert alle Dienste eines Gerätes, während man mit `sdptool search <Dienstekürzel>` nach einem bestimmten Dienst suchen kann. Dieser Aufruf befragt alle erreichbaren

Geräte nach dem gewünschten Dienst. Wird er von einem der Geräte angeboten, so gibt das Programm den vom Gerät gelieferten (vollen) Dienstnamen und eine kurze Beschreibung dazu aus. Eine Liste aller möglichen Dienstkürzel erhält man durch Aufruf von `sdptool` ohne irgendwelche Parameter.

16.4.5 Beispiele

Um zu zeigen, was mit Bluetooth alles möglich ist, sind nachstehend zwei Beispiele aufgeführt.

Netzwerkverbindung zwischen zwei Rechnern R1 und R2

Im ersten Beispiel soll eine Netzwerkverbindung zwischen zwei Rechnern aufgebaut werden. Dies geschieht mit Hilfe des pand (*Personal Area Networking*). Die nachstehenden Kommandos müssen vom Benutzer `root` durchgeführt werden. Auf eine genauere Erläuterung der Netzwerkkommandos (ip) wird verzichtet und nur auf die Bluetooth bedingten Aktionen eingegangen:

Auf einem der beiden Rechner (im folgenden als *R1* bezeichnet) wird der pand mit dem Kommando `pand -s` gestartet. Auf dem zweiten Rechner *R2* wird mittels `hcitool inq` dessen Geräteadresse ermittelt. Mit `pand -c <Geräteadresse>` kann dann eine Verbindung aufgebaut werden. Ruft man jetzt eine Liste der zur Verfügung stehenden Netzwerkschnittstellen mit `ip link show` auf, so sollte ein Eintrag in der Form:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

zu finden sein (an Stelle von `00:12:34:56:89:90` sollte die lokale Geräteadresse stehen). Dieser Schnittstelle muss jetzt eine IP-Adresse zugewiesen werden, und sie in den aktiven Zustand gebracht werden.

Dies geschieht z.B. durch die beiden Kommandos (auf *R1*)

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

bzw. analog auf *R2*

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Bitte beachten Sie, die 3 ist jetzt eine 4. *R1* ist damit von *R2* unter der IP `192.168.1.3` erreichbar. Mit `ssh 192.168.1.4` können Sie sich jetzt von *R1* aus einloggen (sofern *R2* einen sshd, wie er standardmässig unter SUSE LINUX läuft, im Betrieb hat). Der Aufruf `ssh 192.168.1.4` funktioniert im übrigen jetzt auch als „normaler“ Benutzer.

Datentransfer vom Mobiltelefon auf den Rechner

Im zweiten Beispiel soll ein mit einem Fotomobiltelefon erzeugtes Bild (ohne zusätzliche Kosten z.B. durch den Versand einer Multimediamail zu erzeugen) auf einen Rechner transportiert werden. Bitte beachten Sie, dass jedes Mobiltelefon eine andere Menüstruktur besitzt, aber die Vorgehensweise meist ähnlich ist. Konsultieren Sie nötigenfalls die Anleitung für Ihr Telefon. Nachstehend wird der Transfer eines Bildes von einem Sony Ericsson auf einen Laptop beschrieben. Dazu muss einerseits auf dem Rechner der Dienst Obex-Push vorhanden sein, andererseits der Rechner auch dem Mobiltelefon den Zugriff erlauben. Im ersten Schritt wird der Dienst auf dem Laptop zur Verfügung gestellt. Dies geschieht mit dem Daemon opd, der aus dem Paket `bluez-utils` kommt. Starten Sie diesen mit:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Wichtig sind dabei zwei Parameter. `--sdp` meldet den Dienst beim sdpd an. Der Parameter `--path /tmp` teilt dem Programm mit, wohin es empfangene Daten speichern soll — in diesem Fall nach `/tmp/`. Genauso können Sie auch andere Pfade angegeben. Sie brauchen nur Schreibberechtigung im angegebenen Verzeichnis.

Jetzt muss das Mobiltelefon den Rechner „kennenlernen“. Suchen Sie dazu das Menü ‘Verbindungen’ auf dem Telefon auf, und wählen Sie dort ‘Bluetooth’ an. Gehen Sie gegebenenfalls auf ‘Einschalten’, bevor Sie den Punkt ‘Eigene Geräte’ auswählen. Wählen Sie ‘Neues Gerät’ aus und lassen Sie Ihr Telefon nach dem Laptop suchen. Wenn ein Gerät gefunden wird, so erscheint es mit seinem Namen im Display. Wählen Sie das zum Laptop gehörende Gerät aus. Jetzt sollte eine PIN-Abfrage kommen, bei der Sie bitte den PIN aus `/etc/bluetooth/pin` eingeben. Damit kennt das Telefon jetzt den Laptop, und kann mit diesem auch Daten austauschen. Verlassen Sie jetzt das Menü und suchen Sie das Bildermenü auf. Wählen Sie ein Bild aus, dass Sie transferieren möchten und drücken Sie dann den ‘Mehr’-Button. Im jetzt erscheinenden Menü kommen Sie über ‘Senden’ zu einer Auswahl wie Sie es verschicken möchten. Wählen Sie ‘Über Bluetooth’ aus. Jetzt sollte der Laptop als Zielgerät selektierbar sein. Nach der Auswahl

des Rechners erfolgt die Übertragung, und das Bild wird in das beim Aufruf des opd angegebene Verzeichnis gelegt. Genauso könnte Sie natürlich ein Musikstück auf den Laptop übertragen.

16.4.6 Troubleshooting

Bei Verbindungsproblemen empfiehlt es sich, folgende Liste abzuarbeiten:

- Überprüfen Sie die Ausgabe von `hcitool dev`. Wird das lokale Gerät angezeigt? Wenn nicht, ist entweder der hcid nicht gestartet, oder das Gerät wird nicht als Bluetooth-Gerät erkannt (entweder weil der Treiber dies nicht kann oder weil das Gerät kaputt ist). Starten Sie den Daemon mit `rcbluetooth restart` neu und werfen Sie einen Blick in `/var/log/messages`, ob irgendwelche Fehler aufgetreten sind.
- „Sieht“ der Rechner andere Geräte wenn Sie `hcitool inq` aufrufen? Probieren Sie das ruhig zweimal, evtl. war die Verbindung nicht ganz in Ordnung. Das Frequenzband für Bluetooth wird auch von anderen Geräten benutzt.
- Überprüfen Sie, ob die PIN in `/etc/bluetooth/pin` und die PIN des anderen Gerätes übereinstimmen.
- Versuchen Sie, die Verbindung vom anderen Gerät aus zu initiieren. Überprüfen Sie, ob dieses Gerät den Rechner sieht.
- Das erste Beispiel (Netzwerkverbindung) klappt nicht. Hier gibt es verschiedene Problemmöglichkeiten: Zum einen kann es sein, dass einer der beiden Rechner das ssh-Protokoll nicht versteht. Probieren Sie, ob `ping 192.168.1.3` bzw. `ping 192.168.1.4` klappt. Wenn ja überprüfen Sie, ob der sshd läuft. Ein anderes Problem kann sein, dass Sie bereits andere Adressen haben, die mit den im Beispiel genannten `192.168.1.X` Konflikte erzeugen. Versuchen Sie einfach andere Adressen, z.B. `10.123.1.2` und `10.123.1.3`.
- Im zweiten Beispiel erscheint der Laptop nicht als Zielgerät: Erkennt das Mobilgerät den Dienst Obex-Push auf dem Laptop? Gehen Sie dazu im ‘Eigene Geräte’-Menü zum betreffenden Gerät, und lassen Sie sich die ‘Dienstliste’ anzeigen. Steht hier (auch nach dem Aktualisieren der Liste) kein Obex-Push, so liegt das Problem am opd auf dem Laptop. Ist der opd gestartet? Haben Sie Schreibberechtigung auf das angegebene Verzeichnis?

- Geht das zweite Beispiel auch umgekehrt? Ja, wenn Sie obexftp installiert haben, geht dies mit `obexftp -b <Geräteadresse> -B 10 -p <bild>` auch bei einigen Geräten (Siemens und Sony Ericsson sind getestet, andere können, müssen aber nicht).

16.4.7 Weitere Informationen

Eine gute Übersicht über verschiedene Anleitungen zum Umgang und zur Konfiguration von Bluetooth findet sich unter: `http://www.holtmann.org/linux/bluetooth/`

Gute Informationen und Anleitungen:

- GPRS über Bluetooth (deutschsprachige Seite): `http://www.vanschelve.de/edv-wissen/linux/bluetooth_1.htm`
- Verbindung mit PalmOS PDA (englischsprachige Seite): `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

Offizielles Howto für den im Kernel integrierten *Bluetooth Protocol Stack*: `http://bluez.sourceforge.net/howto/index.html`

Powermanagement

Dieses Kapitel bietet einen Überblick über die verschiedenen Powermanagement-Techniken unter Linux. Die Konfiguration aller einsetzbaren Techniken von APM (engl. *Advanced Power Management*) über ACPI (engl. *Advanced Configuration and Power Interface*) bis hin zum CPU Frequency Scaling werden hier detailliert beschrieben.

► **S/390, zSeries**
Die in diesem Kapitel beschriebenen Funktionen und Hardware existieren auf IBM S/390 und zSeries nicht. Das Kapitel ist für diese Plattformen nicht relevant. ◄

17.1 Stromsparfunktionen 394
17.2 APM 396
17.3 ACPI 399
17.4 Pause für die Festplatte 405
17.5 Das powersave Paket 407
17.6 Das YaST Powermanagement-Modul 413
17.7 WOL – Wake on Lan 416

Vom reinen Powermanagement auf Laptops mit APM ist die Entwicklung weitergegangen in Richtung ACPI, das ein auf allen modernen Rechnern (Laptops, Desktops und Servern) verfügbares Hardwareinformations- und -konfigurationswerkzeug darstellt. Auf vielen modernen Hardwaretypen kann ausserdem die CPU-Frequenz der Situation entsprechend angepasst werden, was gerade bei mobilen Geräten kostbare Akkulaufzeit einsparen hilft (*CPU Frequency Scaling*).

Alle Powermanagement-Techniken setzen eine dafür ausgelegte Hardware und passende BIOS-Routinen voraus. Die meisten Notebooks und viele moderne Desktops und Server bringen diese Voraussetzungen mit. Auf älterer Hardware wurde oft APM verwendet (engl. *Advanced Power Management*). Da APM im Wesentlichen aus einem im BIOS implementierten Satz von Funktionen besteht, ist die APM-Unterstützung auf unterschiedlicher Hardware unter Umständen unterschiedlich gut. ACPI ist wesentlich komplexer und variiert in der Unterstützung durch die Hardware noch stärker als APM. Aus diesem Grund macht es keinen Sinn, die Verwendung des einen oder anderen Systems zu propagieren. Testen Sie die unterschiedlichen Verfahren auf Ihrer Hardware und nutzen Sie die Technologie, die am besten unterstützt wird.

Hinweis

Powermanagement auf AMD64-Prozessoren

Die AMD64-Prozessoren unterstützen mit einem 64-bit Kernel ausschließlich ACPI.

Hinweis

17.1 Stromsparfunktionen

Viele dieser Funktionen sind von allgemeinem Interesse, aber so richtig wichtig sind diese vor allem im mobilen Einsatz. Im Folgenden werden diese Funktionen beschrieben und erklärt von welchem System diese ausgeführt werden können.

Stand-by In dieser Betriebsart wird nur das Display ausgeschaltet und bei manchen Geräten die Prozessorleistung gedrosselt. Nicht jede APM-Implementierung stellt diese Funktion zur Verfügung. Bei *ACPI* entspricht das dem Zustand *S1*.

Suspend (to memory) Hier wird der gesamte Systemzustand in den Arbeitsspeicher geschrieben und außer diesem das gesamte System

schlafen gelegt. In diesem Zustand braucht der Computer nur sehr wenig Strom, sodass man damit je nach Gerät von zwölf Stunden bis mehrere Tage mit Batterie überbrücken kann. Der Vorteil dieses Zustands ist, dass man innerhalb weniger Sekunden wieder an derselben Stelle weiterarbeiten kann, ohne erst booten und benötigte Programme neu laden zu müssen. Bei den meisten modernen Geräten genügt es, den Deckel zu schließen, um zu suspendieren, und ihn zum Weiterarbeiten einfach wieder zu öffnen. Bei *ACPI* entspricht das dem Zustand *S3*. Die Unterstützung dieses Zustands ist stark hardwareabhängig.

Hibernation (Suspend to disk) In dieser Betriebsart hält es der Computer länger als einen Winter aus (Hibernation bedeutet „Winterschlaf"), denn der Systemzustand wird vollständig auf der Festplatte gespeichert und das System danach ausgeschaltet. Die Rückkehr aus dem „Winterschlaf" dauert zwischen 30 und 90 Sekunden und auch hier wird der Zustand vor dem Suspend genau wiederhergestellt. Einige Hersteller bieten in ihrem APM sinnvolle Mischformen davon an (zum Beispiel RediSafe bei IBM Thinkpads). Hibernation entspricht bei *ACPI* dem Zustand *S4*.

Kontrolle des Akkuzustands Neben der reinen Information über den Ladezustand, ist es auch wichtig, dass etwas unternommen wird, wenn die Energiereserven knapp werden. Diese Kontrollfunktion übernehmen ACPI oder APM.

Automatisches Ausschalten Nach einem Shutdown wird der Computer vollständig ausgeschaltet. Das ist vor allem von Bedeutung, wenn ein automatischer Shutdown ausgeführt wird, kurz bevor der Akku leer ist.

Abschalten von Systemkomponenten
Die wesentliche Komponente, um Energie zu sparen, ist die Festplatte. Je nach Zuverlässigkeit des gesamten Systems kann diese mehr oder weniger lang schlafen gelegt werden. Allerdings steigt das Risiko eines Datenverlusts mit der Länge der Ruhepausen der Platte. Andere Komponenten können via ACPI (zumindest theoretisch) oder dauerhaft im BIOS-Setup deaktiviert werden.

Kontrolle der Prozessorleistung AMDs PowerNow! und Intels SpeedStep sind zwei Konzepte, die darauf ausgelegt sind, den Stromverbrauch des Gesamtsystems zu senken. Hierzu wird der Stromverbrauch der stromhungrigsten Komponente, des Prozessors, gesenkt. Ein angenehmer Nebeneffekt der reduzierten Prozessorleistung ist eine gerin-

gere Wärmeentwicklung, sodass auch regelbare Lüfter leiser arbeiten können. Die *CPU Frequency Scaling*-Funktionen des Linux-Kernels steuern dies. Hierbei werden im Wesentlichen drei verschiedene Level der Prozessorleistung unterschieden:

performance höchstmögliche Leistung des Prozessors — sinnvoll, wenn das System am Stromnetz betrieben wird.

powersave geringstmögliche Prozessorleistung für den Akkubetrieb

dynamic dynamische Anpassung der Prozessorleistung an die aktuelle Prozessorauslastung — bevorzugte Einstellung sowohl im Akkubetrieb als auch am Netz, um die Batterie zu schonen, Lärm zu vermeiden und bestmögliche Performance zu erreichen. Die Umschaltung zwischen den Frequenzen/Zuständen erfolgt in der Regel so nahtlos, dass der Benutzer im normalen Betrieb nichts davon mitbekommt.

Mehr Informationen zur Kontrolle der Prozessorleistung in Abschnitt 17.5 auf Seite 407.

17.2 APM

Einige der Stromsparfunktionen führt das APM-BIOS selbstständig aus. Stand-by und Suspend kann man auf vielen Notebooks mit Tastenkombinationen oder mit Schließen des Deckels aktivieren. Dazu ist erstmal keinerlei Funktion seitens des Betriebssystems nötig. Wer diese Betriebsarten jedoch per Kommando einleiten möchte, ist darauf angewiesen, dass vor dem Suspend noch bestimmte Aktionen ausgeführt werden. Wer ausserdem einfach nur den Ladezustand der Batterie angezeigt bekommen möchte, muss entsprechende Pakete und einen geeigneten Kernel installiert haben.

Bei den fertigen Kernels von SUSE LINUX ist der APM-Support fest eingebaut, wird aber nur aktiviert, falls kein ACPI im BIOS implementiert ist und ein APM-BIOS gefunden wird. Um den APM-Support einzuschalten, muss ACPI am Bootprompt mit `acpi=off` ausgeschaltet werden. Ob APM aktiviert wurde, lässt sich leicht mit dem Kommando `cat /proc/apm` nachprüfen. Wenn hier eine Zeile mit diversen Zahlen erscheint, ist alles in Ordnung. Jetzt sollte ein `shutdown -h` zum Ausschalten des Computers führen.

Da manche BIOS-Implementierungen sich nicht exakt an Standards halten, kommt es manchmal zu merkwürdigem Verhalten. Manche Probleme kann

man mit speziellen Bootparametern umgehen (früher waren dies Kernelkonfigurationsoptionen). Alle Parameter werden am Bootprompt in der Form `apm=<parameter>` eingegeben:

on/off APM Support ein- oder ausschalten

(no-)allow-ints Während des Ausführens von BIOS-Funktionen Interrupts zulassen.

(no-)broken-psr BIOS hat eine nicht ordnungsgemäß funktionierende „GetPowerStatus"-Funktion.

(no-)realmode-power-off Den Prozessor vor dem Shutdown in den Real Mode zurückschalten.

(no-)debug APM Ereignisse im Syslog protokollieren.

(no-)power-off Nach dem Shutdown das System ausschalten.

bounce-interval=⟨*n*⟩ Zeit in 1/100 Sekunden, in der nach einem Suspendereignis weitere Suspendereignisse ignoriert werden.

idle-threshold=⟨*n*⟩ Prozentsatz der Systeminaktivität, ab der die BIOS-Funktion `idle` aufgerufen wird (0=immer, 100=nie).

idle-period=⟨*n*⟩ Zeitraum in 1/100 Sekunden, über dem die System(in)aktivität ermittelt wird.

17.2.1 Der APM-Daemon (apmd)

Der Daemon `apmd` dient zur Überwachung der Batterie und kann bestimmte Aktionen auslösen, wenn ein Stand-by- oder Suspend-Ereignis eintritt. Er befindet sich im Paket `apmd`. Er ist nicht unbedingt zum Betrieb notwendig, kann jedoch bei manchen Problemen recht nützlich sein.

Der `apmd` wird nicht automatisch beim Booten gestartet. Ist dies jedoch erforderlich, kann man mit dem YaST Runlevel-Editor die Einstellungen zu den Systemdiensten verändern. Alternativ kann auch das Programm `chkconfig` verwendet werden. Manuell kann er mit dem Kommando `rcapmd start` gestartet werden.

Zur Konfiguration gibt es in `/etc/sysconfig/powermanagement` einige Variablen. Die Datei ist mit Kommentaren versehen, deshalb werden hier nur einige Hinweise gegeben.

APMD_ADJUST_DISK_PERF Damit wird veranlasst, dass das Verhalten der Festplatte an den Zustand der Stromversorgung angepasst wird. Dazu gibt es eine Reihe weiterer Variablen, die entweder mit `APMD_BATTERY` oder `APMD_AC` beginnen. Die ersteren enthalten die Einstellungen für den Batteriebetrieb, die letzteren die für den Betrieb mit externer Stromversorgung.

APMD_BATTERY/AC_DISK_TIMEOUT
Die Zeit von Platteninaktivität, nach der diese angehalten wird. Die Werte sind im Abschnitt 17.4 auf Seite 405 oder in der Manualpage zu `hdparm`, Option `-S`, beschrieben.

APMD_BATTERY/AC_KUPDATED_INTERVAL
Die Zeit zwischen zwei Läufen des Kernel Update Deamons.

APMD_BATTERY/AC_DATA_TIMEOUT
Das maximale Alter gepufferter Daten.

APMD_BATTERY/AC_FILL_LEVEL
Der maximale Füllstand des Festplattenpuffers.

APMD_PCMCIA_EJECT_ON_SUSPEND
Obwohl PCMCIA mit APM-Unterstützung übersetzt ist, gibt es hier manchmal Schwierigkeiten. Einige der Kartentreiber kehren von einem Suspend nicht ordentlich zurück `xirc2ps_cs`. Deshalb kann der apmd das PCMCIA-System vor dem Suspend deaktivieren und danach wieder aktivieren. Dazu wird die Variable `APMD_PCMCIA_EJECT_ON_SUSPEND` auf `yes` gesetzt.

APMD_INTERFACES_TO_STOP Hier können Netzwerk-Interfaces eingetragen werden, die vor dem Suspendieren angehalten und danach wieder gestartet werden sollen.

APMD_INTERFACES_TO_UNLOAD
Wenn außerdem noch die Treibermodule dieser Interfaces entladen werden müssen, ist diese Variable zu verwenden.

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND
Machmal kommt es auch vor, dass das Wiederaufwachen nach einem Suspend nicht funktioniert, wenn ein IDE-Gerät (Festplatte) noch im DMA-Modus ist.

Es gibt noch weitere Möglichkeiten, wie zum Beispiel Tastaturwiederholrate oder die Uhrzeit nach einem Suspend zu korrigieren oder den Laptop automatisch herunterzufahren, wenn das APM-BIOS ein „Batterie

kritisch“-Ereignis sendet. Wer noch speziellere Aktionen ausführen möchte, der kann das Skript `/usr/sbin/apmd_proxy`, das die oben aufgeführten Jobs ausführt, an seine Bedürfnisse anpassen.

17.2.2 Weitere Befehle

Im apmd sind noch einige nützliche Programme enthalten. Mit `apm` kann die aktuelle Batteriekapazität abgefragt werden und das System in Standby (`apm -S`) oder Suspend (`apm -s`) geschickt werden; vgl. die Manualpage von `apm`. Das Kommando `apmsleep` suspendiert das System für eine vorgegebene Zeit. Wer eine Logdatei beobachten möchte, ohne die Festplatte ständig am Laufen zu halten, der kann `tailf` als Ersatz für `tail -f` verwenden.

Natürlich gibt es auch hier Tools für das X Window System. Ebenfalls im apmd findet man xapm, was den Ladezustand der Batterie grafisch anzeigt. Wer den KDE-Desktop verwendet – oder zumindest kpanel –, kann sich auch von kbatmon den Ladestand des Akkus anzeigen lassen und das System suspendieren. Als Alternative ist auch xosview interessant.

17.3 ACPI

ACPI steht für *Advanced Configuration and Power Interface* und soll dem Betriebssystem ermöglichen, die einzelnen Hardwarekomponenten individuell einzurichten und zu steuern. Damit ersetzt ACPI sowohl „Plug and Play“, als auch APM. Weiterhin stellt ACPI noch diverse Informationen über Batterie, Netzteil, Temperatur und Lüfter zur Verfügung und unterrichtet über Systemereignisse, wie zum Beispiel „Deckel schließen“ oder „Batterieladung niedrig“.

Das BIOS stellt Tabellen zur Verfügung, in denen Informationen über die Einzelkomponenten und Methoden für den Zugriff auf die Hardware enthalten sind. Diese Informationen werden vom Betriebssystem verwendet, um zum Beispiel Interrupts zuzuweisen oder Komponenten bedarfsweise an- und abzuschalten. Da das Betriebssystem allerdings Anweisungen ausführt, die im BIOS abgelegt sind, ist man auch hier wieder von der Implementierung des BIOS abhängig. In `/var/log/boot.msg` findet man die Bootmeldungen. Dort meldet ACPI, welche Tabellen es gefunden hat und erfolgreich auslesen konnte. Mehr Information zum Troubleshooting bei ACPI-Problemen lesen Sie unter Abschnitt 17.3.4 auf Seite 403.

17.3.1 Praxis

Wenn der Kernel beim Booten ein ACPI-BIOS erkennt, wird ACPI automatisch aktiviert (und APM deaktiviert). Der Bootparameter `acpi=on` kann höchstens bei älteren Maschinen notwendig sein. Natürlich muss der Computer ACPI 2.0 oder neuer unterstützen. Ob ACPI aktiviert wurde, kann in den Bootmeldungen des Kernels in `/var/log/boot.msg` nachgesehen werden. Es gibt dann auch ein Verzeichnis `/proc/acpi/`, welches im weiteren Verlauf beschrieben wird.

Danach müssen jedoch noch eine Reihe von Modulen geladen werden. Diese werden vom Startskript des ACPI-Daemons geladen. Wenn eines dieser Module Probleme bereitet, kann es in `/etc/sysconfig/powersave/common` vom Laden bzw. Entladen ausgeschlossen werden. Im Systemlog (`/var/log/messages`) findet man die Meldungen der Module und kann sehen, welche Komponenten erkannt wurden.

Jetzt findet man unter `/proc/acpi/` eine Reihe von Dateien, die über den Systemzustand informieren oder mit deren Hilfe man einige Zustände aktiv verändern kann. Allerdings funktioniert hier noch längst nicht alles, weil es sich noch in der Entwicklung befindet, und von der Implementierung des Herstellers abhängt.

Alle Dateien (außer `dsdt` und `fadt`) können mit `cat` gelesen werden. In einigen kann man Einstellungen verändern, indem man mit `echo X <datei>` geeignete Werte für X übergibt (alles unter `/proc` ist nicht wirklich eine Datei auf der Festplatte sondern, eine Schnittstelle zum Kernel). Im Folgenden werden die wichtigsten Dateien beschrieben:

`/proc/acpi/info` Allgemeine Information über ACPI

`/proc/acpi/alarm` Hier lässt sich einstellen, wann das System aus einem Schlafzustand zurückkehrt. Momentan ist dieses Feature noch nicht hinreichend unterstützt.

`/proc/acpi/sleep` Gibt Auskunft über die möglichen Schlafzustände.

`/proc/acpi/event` Hier werden alle Ereignisse gemeldet. Diese werden von einem Daemon wie `acpid` oder `powersaved` verarbeitet. Wenn kein Daemon darauf zugreift, kann man die Ereignisse mit `cat /proc/acpi/event` lesen (Mit Strg + C beenden). Ein kurzer Druck auf die Powertaste oder das Schließen des Deckels sind solche Ereignisse.

/proc/acpi/dsdt und /proc/acpi/fadt
Hierin stehen die ACPI-Tabellen DSDT (*Differentiated System Description Table*) und FADT (*Fixed ACPI Description Table*). Diese können mit `acpidmp`, `acpidisasm` und `dmdecode` ausgelesen werden. Diese Programme einschließlich Dokumentation finden Sie im Paket `pmtools`. Beispiel: `acpidmp DSDT | acpidisasm`.

/proc/acpi/ac_adapter/AC/state
Ist das Netzteil angeschlossen?

/proc/acpi/battery/BAT*/{alarm,info,state}
Ausführliche Information über den Zustand der Batterien. Um den Füllstand ablesen zu können, muss `last full capacity` aus `info` mit `remaining capacity` aus `state` verglichen werden. Komfortabler geht das mit speziellen Programmen, die nachher beschrieben werden. In `alarm` kann die Kapazität eingegeben werden, bei der ein Batterieereignis ausgelöst wird.

/proc/acpi/button In diesem Verzeichnis gibt es Informationen über diverse Schalter.

/proc/acpi/fan/FAN/state Dies zeigt an, ob der Lüfter gerade läuft. Er kann auch manuell ein- und ausgeschaltet werden, indem man 0 (=ein) bzw. 3 (=aus) in diese Datei schreibt. Es ist jedoch zu beachten, dass sowohl der ACPI-Code im Kernel als auch die Hardware (bzw. das BIOS) diese Einstellung überschreiben, wenn es zu warm wird.

/proc/acpi/processor/CPU*/info
Informationen über die Energiesparmöglichkeiten des Prozessors.

/proc/acpi/processor/CPU*/power
Information über den gegenwärtigen Prozessorzustand. Ein Sternchen bei 'C2' bedeutet Leerlauf; das ist der häufigste Zustand, wie an der Zahl `usage` zu Erkennen ist.

/proc/acpi/processor/CPU*/performance
Diese Schnittstelle wird nicht mehr verwendet.

/proc/acpi/processor/CPU*/throttling
Hier ist eine weitere lineare Drosselung des Prozessors möglich. Diese Schnittstelle ist veraltet. Ihre Funktion haben die Einstellungen unter `/etc/sysconfig/powersave/common` übernommen (siehe Abschnitt 17.5.2 auf Seite 409).

/proc/acpi/processor/CPU*/limit
Wenn Performance und Throttling von einem Daemon automatisch geregelt werden, lassen sich hier die Grenzen angeben, die nicht überschritten werden dürfen. Es gibt vom System festgelegte Limits und solche, die vom Benutzer einstellbar sind. Ihre Funktion haben die Einstellungen unter `/etc/sysconfig/powersave/common` übernommen (siehe Abschnitt 17.5.2 auf Seite 409).

/proc/acpi/thermal_zone/ Hier gibt es für jede Thermalzone ein Unterverzeichnis. Eine Thermalzone ist ein Bereich mit ähnlichen thermischen Eigenschaften, deren Anzahl und Namen vom Hardware-Hersteller gewählt werden. Viele der Möglichkeiten, die ACPI bietet, werden jedoch nur selten implementiert. Stattdessen, wird die Temperatursteuerung auf herkömmliche Weise direkt vom BIOS übernommen, ohne dem Betriebssystem ein wesentliches Mitspracherecht einzuräumen, denn es geht um nicht weniger als die Lebensdauer der Hardware. Die folgenden Beschreibungen sind also teilweise theoretischer Natur.

/proc/acpi/thermal_zone/*/temperature
Die aktuelle Temperatur der Thermalzone.

/proc/acpi/thermal_zone/*/state
Der Status sagt aus, ob alles „ok“ ist oder ob ACPI „aktiv“ oder „passiv“ kühlt. Bei ACPI-unabhängiger Lüftersteuerung ist hier immer alles „ok“.

/proc/acpi/thermal_zone/*/cooling_mode
Hier kann man unter voller ACPI-Kontrolle die bevorzugte Kühlmethode wählen. Entweder passiv (weniger Leistung, aber sparsam) oder aktiv (immer volle Leistung und voller Lüfterlärm).

/proc/acpi/thermal_zone/*/trip_points
Hier kann eingestellt werden, ab welcher Temperatur etwas unternommen werden soll. Das reicht von passiver oder aktiver Kühlung über Suspendierung („hot“) bis zum Abschalten des Computers („critical“).

/proc/acpi/thermal_zone/*/polling_frequency
Wenn der Wert in `temperature` nicht automatisch aktualisiert wird, sobald sich die Temperatur ändert, kann hier auf den „Polling Modus“ umgeschaltet werden. Der Befehl `echo X > /proc/acpi/thermal_zone/*/polling_frequency` bewirkt, dass die Temperatur alle X Sekunden abgefragt wird. Mit X=0 wird das „Polling“ wieder ausgeschaltet.

17.3.2 Der ACPI-Daemon (acpid)

Ähnlich wie der APM Daemon verarbeitet der ACPI Daemon bestimmte ACPI Ereignisse. Diese sind zur Zeit lediglich die Bestätigung bestimmter Schalter wie der Ein/Aus-Schalter oder der Deckelkontakt. Alle Ereignisse werden im Systemlog protokolliert. In `/etc/sysconfig/powermanagement` kann in den Variablen `ACPI_BUTTON_POWER` und `ACPI_BUTTON_LID` festgelegt werden, was bei diesen Ereignissen geschehen soll. Wem das nicht genügt, der kann das Skript `/usr/sbin/acpid_proxy` anpassen oder die Konfiguration des `acpid` unter `/etc/acpi/` verändern.

Im Gegensatz zum `apmd` ist hier nicht sehr viel vorkonfiguriert, da sich ACPI unter Linux noch stark entwickelt. Bei Bedarf muss man sich den `acpid` selbst zurecht konfigurieren. Für Vorschläge zu vorbereiteten Aktionen sind wir jederzeit unter `http://www.suse.de/feedback` zu erreichen.

17.3.3 Weitere Tools

Es gibt eine Reihe von mehr oder weniger umfangreichen ACPI-Werkzeugen. Darunter reine Informationstools, die Batteriezustand, Temperatur usw. anzeigen (acpi, klaptopdaemon, wmacpimon etc.). Andere vereinfachen den Zugriff auf die Strukturen unter `/proc/acpi` oder helfen Veränderungen zu beobachten (akpi, acpiw, gtkacpiw). Des weiteren gibt es noch Werkzeuge zum Bearbeiten der ACPI Tabellen im BIOS (Paket `pmtools`).

17.3.4 Mögliche Probleme und Lösungen

Es gibt zwei unterschiedliche Gruppen von Problemen. Einerseits können natürlich Fehler im ACPI-Code des Kernels enthalten sein, die nicht rechtzeitig bemerkt wurden. Dann wird es jedoch eine Lösung zum Download geben. Unangenehmer und leider auch häufiger sind Probleme im BIOS eines Computers. Es kommt leider sogar vor, dass Abweichungen von der ACPI-Spezifikation im BIOS eingebaut werden, um Fehler der ACPI-Implementierung in anderen sehr verbreiteten Betriebssystemen zu umgehen. Es gibt auch Hardware, bei der gravierende Fehler in der ACPI-Implementierung bekannt sind und die deshalb in einer Blacklist vermerkt sind, damit der Linuxkernel ACPI dort nicht verwendet.

Falls ein Problem auftritt, sollte man also zunächst das BIOS aktualisieren. Viele Probleme lösen sich dabei einfach in Luft auf. Falls der Rechner überhaupt nicht vernünftig bootet, hilft eventuell einer der folgenden Bootparameter:

pci=noacpi Kein ACPI zur Konfiguration der PCI-Geräte verwenden.

acpi=oldboot Nur einfache Ressourcenkonfiguration durchführen, sonst ACPI nicht verwenden.

acpi=off Kein ACPI verwenden.

Achtung

Probleme beim Booten ohne ACPI

Manche Rechner der neueren Generation, insbesondere SMP-Systeme und AMD64-Systeme benötigen ACPI für eine korrekte Hardwarekonfiguration. Ein Abschalten von ACPI kann zu Problemen führen.

Achtung

Wichtig ist dann jedenfalls, sich die Bootmeldungen genauer anzusehen. Am besten verwendet man dafür nach dem Booten das Kommando `dmesg | grep -2i acpi` (oder auch alle Meldungen, denn das Problem muss ja nicht an ACPI hängen). Wenn ein Fehler beim Parsen einer ACPI Tabelle auftritt, gibt es zumindest für die wichtigste Tabelle, die DSDT, die Möglichkeit, dem System eine verbesserte Version unterzuschieben. Dann wird die fehlerhafte DSDT des BIOS ignoriert. Das Vorgehen wird unter Abschnitt 17.5.4 auf Seite 411 näher beschrieben.

Es gibt bei der Kernelkonfiguration auch einen Schalter, um Debug-Meldungen von ACPI zu aktivieren. Wenn man sich einen Kernel mit ACPI Debugging kompiliert und installiert hat, kann man Experten, die einen Fehler suchen, mit detaillierter Information unterstützen.

Auf alle Fälle ist es bei BIOS- oder Hardwareproblemen immer eine gute Idee, sich an den Hersteller des Gerätes zu wenden. Auch wenn diese einem bei Linux nicht immer weiterhelfen können, ist es jedoch von Bedeutung, dass diese den Begriff Linux so häufig als möglich hören. Erst wenn die Hersteller merken, dass genug ihrer Kunden Linux verwenden, werden sie es ernst nehmen. Es schadet auch nichts, wenn Sie ohne Probleme dem Hersteller Ihrer Hardware erzählen, dass Sie Linux darauf verwenden.

Weitere Dokumentation und Hilfe finden Sie unter:

- c't 2002, Heft 25: Schöne neue Welt (Dominik Brodowski, Oliver Diedrich)
- `http://www.cpqlinux.com/acpi-howto.html` (etwas genaueres ACPI HowTo, enthält Patches der DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (ACPI FAQ @Intel)
- `http://acpi.sourceforge.net/` (Das ACPI4Linux-Projekt bei Sourceforge)
- `http://www.poupinou.org/acpi/` (DSDT Patches von Bruno Ducrot)

17.4 Pause für die Festplatte

Man kann unter Linux die Festplatte abschalten, wenn sie nicht benötigt wird. Dazu dient das Programm hdparm, mit dem man diverse Einstellungen an den Festplatten vornehmen kann. Mit der Option `-y` wird die Platte sofort in den Stand-by-Modus geschickt, mit `-Y` (Vorsicht!) wird sie vollständig abgeschaltet. Mit `hdparm -S <x>` wird erreicht, dass die Platte nach einer bestimmten Zeit Inaktivität abgeschaltet wird. Der Platzhalter $\langle x \rangle$ hat folgende Bedeutung: `0` schaltet diesen Mechanismus aus, die Platte läuft immer. Werte von `1` bis `240` werden mit 5 Sekunden multipliziert. `241` bis `251` entsprechen 1 bis 11 mal 30 Minuten.

Häufig ist es aber nicht ganz so einfach, die Festplatte in den Ruhezustand zu versetzen. Unter Linux gibt es eine Vielzahl von Prozessen, die durch Schreibvorgänge die Platte immer wieder aufwecken. Deshalb ist es an dieser Stelle wichtig zu verstehen, wie Linux mit Daten umgeht, die auf die Platte geschrieben werden sollen. Alle Daten werden zuerst in einen Puffer im Arbeitsspeicher zwischengespeichert. Dieser Puffer wird vom „Kernel Update Daemon" (kupdated) überwacht. Immer wenn Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem gewissen Grad gefüllt ist, wird der Puffer geleert und die Daten der Festplatte übergeben. Die Größe des Puffers ist übrigens dynamisch und hängt von der Speichergröße und der Systemauslastung ab. Da das vorrangige Ziel Datensicherheit ist, wird der kupdated standardmäßig auf kleine Zeitintervalle eingestellt. Er prüft den Puffer alle 5 Sekunden und benachrichtigt den bdflush-Daemon, wenn Daten älter als 30 Sekunden sind oder der Puffer zu 30% gefüllt ist. Der bdflush-Daemon schreibt dann die Daten auf die

Platte. Er schreibt auch unabhängig vom kupdated wenn zum Beispiel der Puffer voll ist. Wer ein stabiles System hat, kann diese Einstellungen nun verändern. Man muss sich jedoch immer darüber im Klaren sein, dass dies auf Kosten der Datensicherheit geht.

Achtung

Beeinträchtigung der Datensicherheit

Änderungen an den Einstellungen des Kernel Update Daemon beeinflussen die Datensicherheit. Wer sich unsicher ist, lässt lieber die Finger davon.

Achtung

Die Einstellungen für den Festplattentimeout, den kupdated-Intervall, den Füllgrad des Puffers und das Alter der Daten können in `/etc/sysconfig/powermanagement` zweifach abgelegt werden: einmal für den Batteriebetrieb und einmal für den Betrieb mit externer Stromversorgung. Die Variablen sind im Abschnitt über den apmd 17.2.1 auf Seite 397 und in der Datei selbst beschrieben. Weiterhin finden Sie einige Information zum Thema unter `/usr/share/doc/packages/powersave`.

Neben all diesen Vorgängen schreiben so genannte „Journaling Dateisysteme“ wie zum Beispiel ReiserFS oder Ext3 unabhängig von bdflush ihre Metadaten auf die Festplatte, was natürlich auch ein Einschlafen der Platte verhindert. Um das zu vermeiden, gibt es jetzt eine Erweiterung im Kernel, die speziell für mobile Geräte entwickelt wurde. Die genaue Beschreibung dazu findet man in `/usr/src/linux/Documentation/laptop-mode.txt`.

Weiterhin ist natürlich zu beachten, wie sich die Programme verhalten, die man gerade verwendet. Zum Beispiel schreiben gute Texteditoren regelmäßig versteckte Sicherungen der gerade geänderten Datei auf die Platte. Das weckt dann die Platte immer wieder auf. Solche Eigenschaften von Programmen können auch abgeschaltet werden, aber auch hier wieder auf Kosten der Datensicherheit.

In diesem Zusammenhang gibt es für den Maildaemon postfix eine Variable `POSTFIX_LAPTOP`. Wenn diese auf `yes` gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu. Das ist jedoch nicht von Bedeutung, wenn das Intervall für den kupdated verlängert wurde.

17.5 Das powersave Paket

Das `powersave` Paket ist hauptsächlich für die Anwendung in Laptops ausgelegt, wo es für die Stromsparfunktion beim Batteriebetrieb zuständig ist. Manche seiner Features sind aber auch für normale Arbeitsplatzrechner und Server interessant (z.B. Suspend/Standby, ACPI-Button-Funktionalität und Abstellen von IDE-Festplatten).

In diesem Paket sind alle Powermanagementfunktionen Ihres Rechners zusammengefasst. Es unterstützt Hardware, die ACPI, APM, IDE-Platten und PowerNow!- bzw. SpeedStep-Technologien nutzt. Die Funktionalitäten aus den Paketen `apmd`, `acpid`, `ospmd` und `cpufreqd` (mittlerweile `cpuspeed`) wird im Paket `powersave` zusammengefasst. Aus diesem Grund sollten Daemonen aus diesen Paketen nicht parallel zum powersave-Daemon betrieben werden.

Selbst wenn Ihr System nicht alle der oben genannten Hardwareelemente enthält (APM und ACPI schließen sich gegenseitig aus), sollten Sie den powersave Daemon zur Regelung der Stromsparfunktion nutzen. Eventuelle Änderungen der Hardwarekonfiguration erkennt der Daemon automatisch.

Hinweis

Informationen zu powersave

Neben diesem Kapitel sind aktuelle Informationen zum powersave Paket auch unter `/usr/share/doc/packages/powersave/README_POWERSAVE` verfügbar.

Hinweis

17.5.1 Konfiguration des powersave Pakets

Generell ist die Konfiguration von powersave über mehrere Dateien verteilt:

`/etc/powersave.conf` Diese Datei wird vom powersave-Daemon benötigt, um die Bearbeitung auftretender Systemereignisse (engl. *Events*) an den powersave_proxy zu delegieren. Darüber hinaus werden hier benutzerdefinierte Einstellungen zum genauen Verhalten des Daemons vorgenommen.

/etc/sysconfig/powersave/common
: Diese Datei dient der allgemeinen Konfiguration des Startupskripts (`rcpowersave`) und des Proxies. Die Voreinstellungen können meistens unverändert übernommen werden.

/etc/sysconfig/powersave/scheme_*
: Dies sind die verschiedenen Schemes oder auch Profile, die die Anpassung des Stromverbrauchs an bestimmte Einsatzszenarien regeln. Einige sind vorkonfiguriert und ohne weitere Änderungen einsatzbereit. Sie können allerdings auch eigene Profile hier ablegen.

17.5.2 Konfiguration von APM und ACPI

Suspend und Standby

In der Datei `/etc/sysconfig/powersave/common` legen Sie fest, welche kritischen Module und Dienste vor einem Suspend- oder Standby-Ereignis entladen bzw. gestoppt werden sollen. Wird das System später wieder hochgefahren, werden diese wieder geladen bzw. gestartet. Die Voreinstellungen betreffen in der Hauptsache USB- und PCMCIA-Module.

POWERSAVE_SUSPEND_RESTART_SERVICES=""
: Listen Sie hier die nach einem Suspend neu zu startenden Dienste auf.

POWERSAVE_STANDBY_RESTART_SERVICES=""
: Listen Sie hier die nach einem Standby neu zu startenden Dienste auf.

POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND=""
: Listen Sie die vor einem Suspend zu entladenden Module auf.

POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
: Listen Sie die vor einem Standby zu entladenden Module auf.

Ausserdem stellen Sie sicher, dass die folgenden Standardoptionen zur korrekten Verarbeitung von Suspend/Standby, Occurrence/Resume gesetzt sind (dies sind normalerweise die Voreinstellungen nach der Installation von SUSE LINUX):

```
POWERSAVE_EVENT_GLOBAL_SUSPEND="prepare_suspend"
POWERSAVE_EVENT_GLOBAL_STANDBY="prepare_standby"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND="restore_after_suspend"
POWERSAVE_EVENT_GLOBAL_RESUME_STANDBY="restore_after_standby"
```

In der Konfigurationsdatei des powersave Daemons unter `/etc/powersave.conf` werden diese Ereignisse dem `powersave_proxy`-Skript zugeordnet, das ausgeführt wird, sobald diese Ereignisse eintreten (Voreinstellung nach der Installation):

```
global.suspend=/usr/sbin/powersave_proxy
global.standby=/usr/sbin/powersave_proxy
global.resume.suspend=/usr/sbin/powersave_proxy
global.resume.standby=/usr/sbin/powersave_proxy
```

Benutzerdefinierte Batteriezustände

Sie können in der Datei `/etc/powersave.conf` drei Ladezustände der Batterie (in Prozent) festlegen, bei deren Erreichen das System warnt bzw. bestimmte Aktionen ausführt.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

Welche Aktionen/Skripte ausgeführt werden, sobald bestimmte Ladezustände unterschritten werden, ist in der Konfigurationsdatei des powersave-Daemons festgelegt (`/etc/powersave.conf`). Der Typ dieser Aktionen ist in `/etc/sysconfig/powersave/common` konfiguriert:

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="suspend"
```

Weitere Optionen lesen Sie direkt in dieser Konfigurationsdatei nach.

Anpassungen des Stromverbrauchs an verschiedene Arbeitsbedingungen

Sie können das Verhalten des Systems von der Art seiner Stromversorgung abhängig machen. So sollte der Stromverbrauch des Systems vermindert werden, wenn das System vom Netz getrennt und per Batterie betrieben wird. Umgekehrt sollte die Performance des Systems automatisch wieder steigen, sobald es sich wieder am Netz befindet. Konkret beeinflussbar sind die CPU-Frequenz, die Stromsparfunktion von IDE-Platten und einige andere Parameter mehr.

In `/etc/powersave.conf` ist die Ausführung bestimmter Aktionen bei Trennung/Anbindung vom Stromnetz an den `powersave_proxy` delegiert. In `/etc/sysconfig/powersave/common` wählen Sie die zu verwendenden Szenarien (genannt „Schemes“ oder „Profile“) fest:

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Die „Schemes“ sind in entsprechenden Dateien unter `/etc/sysconfig/powersave/` abgelegt. Ihr Name setzt sich zusammen aus: `scheme_<Name des Schemas>`. Im Beispiel werden zwei Schemes referenziert: `scheme_performance` und `scheme_powersave`. Vorkonfiguriert werden `performance`, `powersave` und `acoustic` ausgeliefert. Sie können mittels des YaST Powermanagement-Moduls jederzeit existierende Schemata bearbeiten, neue anlegen, bestehende löschen oder deren Zuordnungen zum Stromversorgungszustand ändern.

17.5.3 Zusätzliche ACPI-Features

Sollten Sie ACPI verwenden, können Sie die Reaktion Ihres Systems auf die so genannten „ACPI-Buttons“ (Power, Sleep und „Deckel offen“, „Deckel geschlossen“) steuern. In `/etc/powersave.conf` ist die Ausführung der entprechenden Aktionen an den powersave_proxy delegiert. Die eigentliche Aktion selbst legen Sie in der Datei `/etc/sysconfig/powersave/common` fest. Nähere Erläuterungen zu den einzelnen Optionen entnehmen Sie bitte dieser Konfigurationsdatei.

POWERSAVE_EVENT_BUTTON_POWER="wm_shutdown"
: Wird der Power-Button gedrückt, reagiert das System mit dem Herunterfahren des jeweiligen Windowmanagers (KDE, GNOME, fvwm...).

POWERSAVE_EVENT_BUTTON_SLEEP="suspend"
: Wird der Sleep-Button gedrückt, fällt das System in den Suspend-Modus.

POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"
: Beim Öffnen des Deckels passiert nichts.

POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"
: Wird der Deckel geschlossen, aktiviert sich der Bildschirmschoner.

Wird der Prozessor für eine bestimmte Zeit nicht über ein festgelegtes Maß hinaus beansprucht, können Sie seine Leistung zusätzlich drosseln. Legen Sie mit `POWERSAVED_CPU_LOW_LIMIT` den Level fest, bei dessen dauerhafter Unterschreitung — die Zeitspanne legen Sie in `POWERSAVED_CPU_IDLE_TIMEOUT` fest — die CPU heruntergeregelt wird.

17.5.4 Troubleshooting

Sämtliche Fehler- und Warnmeldungen werden in der Datei `/var/log/messages` protokolliert. Ergibt sich hier auf den ersten Blick kein Hinweis, weisen Sie powersave in der Datei `/etc/sysconfig/powersave/common` über die Variable `DEBUG` an, seine Meldungen etwas detaillierter und ausführlicher zu halten. Erhöhen Sie den Variablenwert hierzu auf 7 oder gar 15 und starten Sie den Daemon neu. Mithilfe der jetzt ausführlicheren Fehlermeldungen in `/var/log/messages` sollten Sie in der Lage sein, den Fehler einzugrenzen. Die folgenden Fragen und Antworten decken die häufigsten Probleme mit powersave ab.

ACPI ist aktiviert, aber die Batteriezustände und Buttons funktionieren nicht so wie konfiguriert

Sollten Sie mit ACPI Probleme bekommen, durchsuchen Sie mit folgendem Befehl die Ausgabe von `dmesg` nach ACPI-spezifischen Meldungen: `dmesg|grep -i acpi`.

Um den Fehler zu beheben, kann ein BIOS-Update notwendig werden. Besuchen Sie daher die Homepage Ihres Laptopherstellers, suchen Sie nach einer aktuelleren BIOS-Version und spielen Sie diese ein. Geben Sie an den Hersteller Ihres Systems weiter, dass er sich an die aktuellste ACPI-Spezifikation halten soll.

Treten die Fehler nach dem BIOS-Update immer noch auf, suchen Sie auf den folgenden Webseiten nach einer aktuelleren DSDT für Ihr System, um die fehlerhafte DSDT-Tabelle in Ihrem BIOS zu ersetzen:

1. Laden Sie die für Ihr System passende DSDT von `http://acpi.sourceforge.net/dsdt/tables` herunter. Stellen Sie sicher, dass die Datei entzippt und kompiliert ist (zu erkennen an der Dateiendung `.aml` (ACPI Machine Language)). Ist dies der Fall, fahren Sie mit Punkt 3 fort.

2. Ist die Dateiendung der heruntergeladenen Tabelle `.asl` (ACPI Source Language), muss sie mit Hilfe von iasl aus dem Paket `pmtools` kompiliert werden. Rufen Sie hierzu `iasl -sa <Datei>.asl`. Die

aktuellste Version von iasl (Intel ACPI Compiler) finden Sie ausserdem unter `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3. Kopieren Sie die Datei `DSDT.aml` an eine beliebige Stelle (wir empfehlen `/etc/DSDT.aml`). Editieren Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an. Starten Sie `mkinitrd` (Paket `mkinitrd`). Wann immer Sie Ihren Kernel deinstallieren und `mkinitrd` verwenden, um eine initrd zu erstellen, wird die angepasste DSDT eingebunden und zur Bootzeit geladen.

CPU Frequency funktioniert nicht

Überprüfen Sie anhand der Kernelquellen (`kernel-source`), ob Ihr Prozessor unterstützt wird und ob Sie eventuell ein bestimmtes Kernelmodul oder eine bestimmte Moduloption verwenden müssen, um CPU-Frequency zu aktivieren. Diese Informationen finden Sie unter `/usr/src/linux/Documentation/cpu-freq/*`. Wenn ein bestimmtes Modul oder eine bestimmte Option nötig sind, konfigurieren Sie dies in der Datei `/etc/sysconfig/powersave/common` über die Variablen `CPUFREQD_MODULE` und `CPUFREQD_MODULE_OPTS`.

Suspend/Standby funktioniert nicht

Es sind mehrere, mit dem Kernel zusammenhängende Probleme bekannt, die auf **ACPI** Systemen Suspend/Standby verhindern:

- Systeme mit mehr als 1 GB RAM unterstützen im Moment (noch) kein Suspend
- Multiprozessorsysteme oder Systeme mit einem P4-Prozessor (mit Hyperthreading) unterstützen momentan kein Suspend.

Der Fehler kann auch in einer fehlerhaften Implementierung Ihrer DSDT (BIOS) liegen. In diesem Fall spielen Sie eine neue DSDT ein.

Auf **ACPI** und **APM** Systemen gilt Folgendes:

Sobald Ihr System versucht, fehlerhafte Module zu entladen, hängt sich der Proxy auf und das Suspendereignis wird niemals getriggert. Der umgekehrte Weg ist auch möglich, wenn Sie Module/Dienste nicht entladen oder stoppen, die einen erfolgreichen Suspend verhindern. In beiden Fällen sollten Sie versuchen, durch Manipulation der folgenden Einstellungen unter `/etc/sysconfig/powersave/common` herauszufinden, welche Module das Problem hervorrufen:

```
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND=""
POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
POWERSAVE_SUSPEND_RESTART_SERVICES=""
POWERSAVE_STANDBY_RESTART_SERVICES=""
```

Unter Verwendung von ACPI erkennt der Powersave-Daemon ein bestimmtes Batterielimit nicht

Unter ACPI kann das Betriebssystem vom BIOS eine Meldung über das Unterschreiten eines bestimmten Ladeniveaus der Batterie anfordern. Der Vorteil dieser Methode ist, dass nicht permanent der Batteriezustand ausgelesen werden muss, was sonst die Performance des Rechners schwächen würde. Trotzdem kann es vorkommen, dass diese Benachrichtigung laut BIOS zwar funktionieren sollte, tatsächlich aber nicht stattfindet, selbst bei Unterschreitung des Limits nicht.

Sollten Sie dies auf Ihrem System beobachten, setzen Sie in der Datei `/etc/powersave.conf` die Variable `POWERSAVED_FORCE_BATTERY_POLLING` auf `yes`, um das Auslesen des Batteriezustands zu erzwingen.

17.6 Das YaST Powermanagement-Modul

Mit Hilfe des YaST Powermanagement-Moduls können Sie alle Einstellungen zum Powermanagement vornehmen, die in den vorangegangenen Abschnitten erläutert wurden.

Nach dem Start des Moduls über das YaST-Kontrollzentrum ('System' → 'Powermanagement') gelangen Sie in die erste Maske des Moduls (siehe Abbildung 17.1 auf der nächsten Seite), in der Sie zur Auswahl der bei bestimmten Betriebszustände — Akkubetrieb oder Betrieb am Stromnetz — zu verwendenden Schemes aufgefordert werden.

Sie können sich an dieser Stelle per Drop-Down-Menü für jeweils eines der bereits existierenden Schemes entscheiden, oder aber über den Button 'Schemes bearbeiten' in eine Übersicht der bereits vorhandenen Schemes gelangen (Abbildung 17.2 auf Seite 415).

In der Schemes-Übersicht selektieren Sie dasjenige Scheme, das Sie ändern möchten und klicken dann auf 'Ändern', um in den Editierdialog zu gelangen (siehe Abbildung 17.3 auf Seite 416). Alternativ können Sie ein neues Scheme erstellen, indem Sie den Button 'Hinzufügen' drücken. In beiden Fällen ist der Folgedialog identisch.

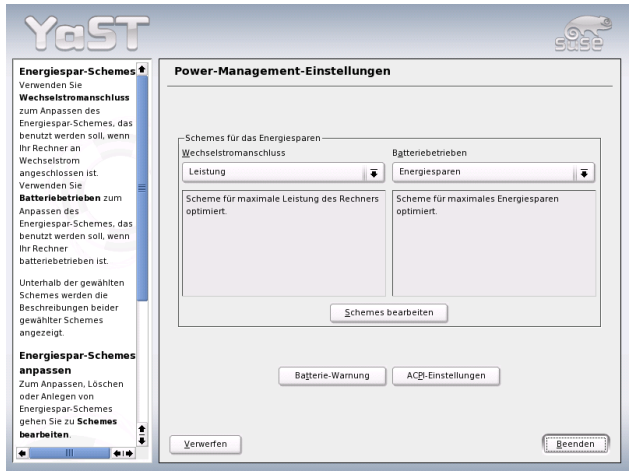

Abbildung 17.1: *YaST-Powermanagement: Scheme selektieren*

Versehen Sie das neue oder zu ändernde Scheme zuerst mit einem (sprechenden) Namen und einer Beschreibung. Für die Festplatte legen Sie eine 'Stand-by-Strategie' fest, die entweder auf maximale Performance oder auf Energieersparnis ausgelegt ist. Die 'Akustik-Strategie' regelt den Geräuschpegel der Festplatte. Klicken Sie auf 'Weiter', um in den Dialog zur Konfiguration der Optionen 'CPU' und 'Kühl-Strategie' zu gelangen. 'CPU' umfasst die Optionen 'Frequenzskalierung' und 'Throttling erlauben', mit deren Hilfe Sie festlegen, ob und inwieweit die CPU-Frequenz bei Bedarf heruntergeregelt werden darf. Die 'Kühl-Strategie' regelt, welche Art der Kühlung angewandt werden soll. Sobald Sie alle Einstellungen für das Scheme abgeschlossen haben, verlassen Sie diesen Dialog mit 'OK' und kehren in den Startdialog (Abbildung 17.1) zurück. Dort können Sie nun das selbsterstellte Scheme für einen der beiden Betriebszustände anwählen. Verlassen Sie diesen Dialog wiederum mit 'OK', werden Ihre Einstellungen aktiv.

Aus dem Startdialog heraus (siehe Abbildung 17.1), können Sie neben der Scheme-Auswahl für verschiedene Betriebszustände auch globale Einstellungen zum Powermanagement vornehmen. Klicken Sie hierzu auf 'Batterie-Warnung' oder 'ACPI-Einstellungen'. Um in den Dialog zum Ladezustand der Batterie zu gelangen, klicken Sie 'Batterie-Warnung' (17.4 auf Seite 417).

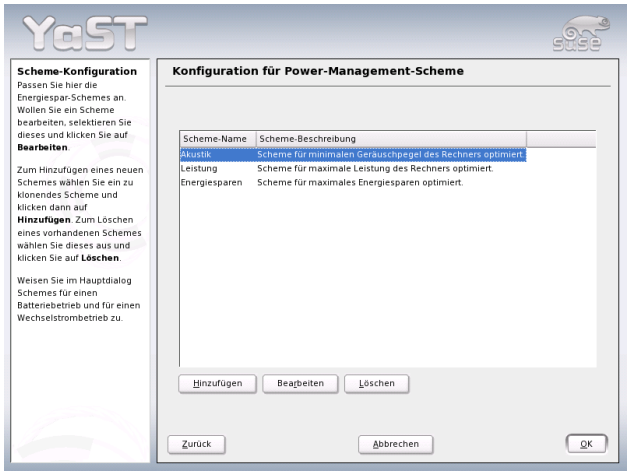

Abbildung 17.2: *YaST-Powermanagement: Überblick der vorhandenen Schemes*

Das BIOS Ihres Systems meldet dem Betriebssystem, sobald bestimmte, konfigurierbare Kapazitätsgrenzen unterschritten werden. Daraufhin können bestimmte Aktionen ausgelöst werden. In diesem Dialog legen Sie drei Grenzen fest, deren Unterschreitung bestimmte Aktionen auslösen soll. Dies sind 'Kapazitätswarnung', 'Niedrige Kapazität' und 'Kritische Kapazität'. In den ersten beiden Fällen wird üblicherweise nur eine Warnmeldung an den Benutzer weitergereicht, während Unterschreitung des letzten kritischen Levels ein Suspend des Rechners auslöst, da die verbliebene Energie kaum noch für längere Zeit einen sinnvollen Betrieb des Systems erlaubt. Wählen Sie die für Ihre Zwecke passenden Ladezustände und entsprechenden Aktionen aus und verlassen Sie diesen Dialog mit 'OK', um zurück in den Startdialog zu gelangen. Von dort aus gelangen Sie über 'ACPI-Einstellungen' in den Dialog zur Konfiguration der ACPI-Buttons (siehe Abbildung 17.5 auf Seite 418).

Mit den Einstellungen zu den ACPI-Buttons legen Sie fest, wie das System auf die Betätigung bestimmter Schalter reagieren soll. Diese Schalter/Ereignisse kennt ACPI als „Buttons". Konfigurieren Sie die Antwort des Systems auf Drücken der (Power)-Taste, einer (Sleep)-Taste und auf Schließen des Laptopdeckels. Mit 'OK' schließen Sie die Konfiguration ab und gelangen zurück in den Startdialog (Abbildung 17.1 auf der vorherigen Seite). Verlassen Sie das gesamte Modul durch ein erneutes Drücken

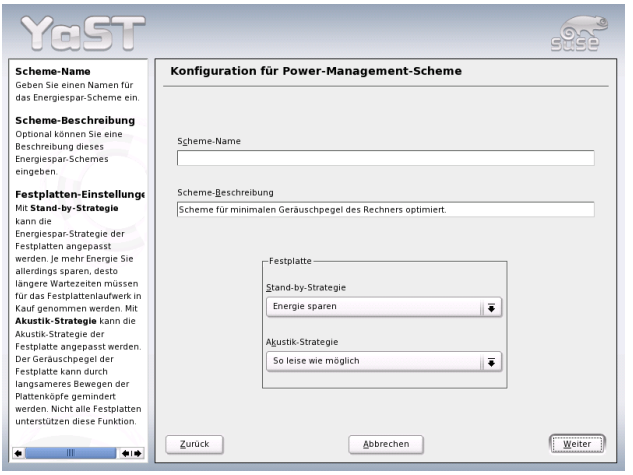

Abbildung 17.3: *YaST-Powermanagement: Scheme erstellen*

von ‘OK’, um alle Ihre Einstellungen zum Powermanagement zu übernehmen.

17.7 WOL – Wake on Lan

WOL (engl. *Wake on Lan*) bezeichnet die Möglichkeit, einen Computer aus dem Stand-by-Modus über ein Netzwerk durch spezielle Pakete „aufzuwecken“. Dieses „Magic Packet“ wird von der Netzwerkkarte empfangen und sorgt dafür, dass das Motherboard die Stromversorgung des Netzteils aktiviert und den Rechner bootet.

Vorteilhaft bei dieser Methode ist, dass Rechner nicht dauerhaft eingeschaltet sein müssen (spart Energie) und trotzdem über WOL aktiviert werden können.

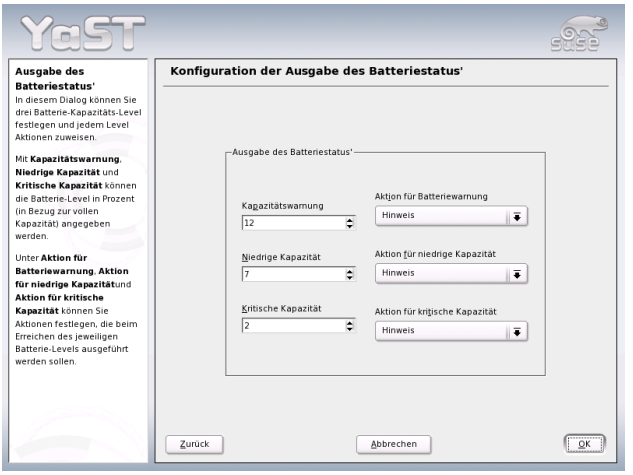

Abbildung 17.4: *YaST-Powermanagement: Ladezustand der Batterie*

Hinweis

Unterstützung von WOL

Wake on Lan funktioniert nur mit neueren Motherboards, die im BIOS diese Funktionalität unterstützen. WOL-fähige Netzwerkkarten enthalten meist Chips der Intel i82557 (EEpro100B), i82558 (EEPro100+) oder i82559-Baureihe. Informieren Sie sich unter `http://support.intel.com/support/network/sb/cs-008459.htm`.
Unglücklicherweise funktioniert manche Hardware nicht, obwohl sie scheinbar WOL-fähig ist. Daher führt leider kein Weg daran vorbei, die entsprechenden Schritte auszuprobieren.

Hinweis

17.7.1 BIOS-Konfiguration

Bevor Sie WOL verwenden, müssen Sie im BIOS eine Option aktivieren, die häufig mit 'OnBoard LAN' oder 'Boot from LAN' beschriftet ist. Sie ist je nach BIOS im Menü 'OnBoard Device Configuration', 'Boot' oder 'PowerSave' zu finden. Konsultieren Sie im zweifelsfalls die Dokumentation zu Ihrem Motherboard.

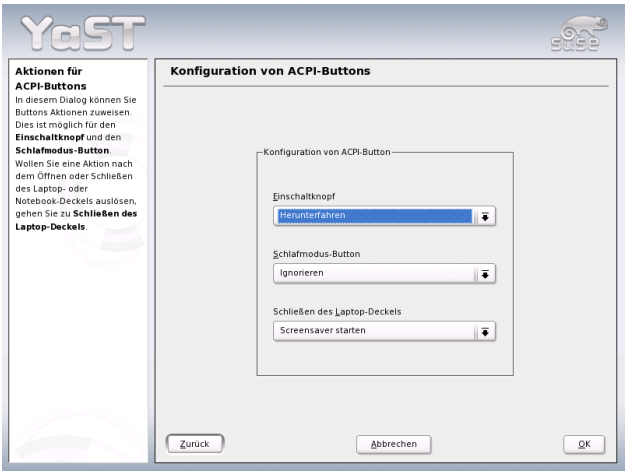

Abbildung 17.5: *YaST-Powermanagement: ACPI-Einstellungen*

Achten Sie ferner darauf, dass Ihr System ein möglichst aktuelles BIOS besitzt und aktualisieren Sie dieses falls nötig. Details zu BIOS-Updates finden Sie auf der Homepage der jeweiligen Motherboardhersteller.

Achtung

BIOS-Update

Ein BIOS-Update ist eine heikle Prozedur. Halten Sie sich daher peinlich genau an die Anweisungen der Motherboard-Hersteller, da sonst Ihr Motherboard funktionsuntüchtig wird und Sie Ihr System nicht mehr hochfahren können.

Achtung

Ältere Netzwerkkarten (zum Beispiel 3COM) müssen mit einem 3poligem Kabel mit dem Motherboard verbunden sein. Bei neueren Netzwerkkarten ist diese Prozedur nicht mehr notwendig.

17.7.2 Einrichtung mit YaST

Starten Sie YaST als Benutzer `root` und rufen Sie unter 'Netzwerkdienste' → 'WOL' das Modul auf. Wenn auf Ihrem Rechner ein DHCP-Server läuft,

zeigt Ihnen das WOL-Modul die vorhandenen Rechner aus Ihrem Netzwerk an, die Sie in Ihre WOL-Liste aufzunehmen können.

Läuft kein DHCP-Server, müssen Sie die entfernten Rechner manuell eintragen. Mittels 'Hinzufügen' geben Sie den Hostnamen und die MAC-Adresse (engl. *Media Access Connector*) der Netzwerkkarte ein. Die MAC-Adresse ist für jedes Netzwerkgerät eindeutig und kann durch folgenden Aufruf angezeigt werden:

```
# ip link show eth0
2: eth0: <BROADCAST,MULTICAST,NOTRAILERS,UP>
mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:80:c8:94:c3:e7 brd ff:ff:ff:ff:ff:ff
```

Tragen Sie den Wert, der hinter 'link/ether' steht, in das Feld 'MAC-Adresse des Clients' ein. Bestätigen Sie mit 'Speichern'. Damit ist die Einrichtung mit YaST abgeschlossen.

17.7.3 Aufwecken von Rechnern

Sind Ihre Rechner eingerichtet, können Sie im WOL-YaST-Modul die Rechner aufwecken, in dem Sie 'Aufwecken' anwählen. Der selektierte Rechner wird dann hochgefahren.

Eine weitere Möglichkeit besteht durch den Befehl `ether-wake` aus dem Paket `netdiag`: Durch Eingabe der MAC-Adresse lässt sich ein bestimmter Rechner aufwecken:

```
# ether-wake 00:80:C8:94:C3:E7
```

Durch `--help` bzw. `-u` erhalten Sie Hilfe zu diesem Befehl.

17.7.4 Weitere Informationen

Weitere Informationen können Sie im Mini HOWTO von WOL unter `http://gsd.di.uminho.pt/jpo/software/wakeonlan/mini-howto/wol-mini-howto.html` finden.

Dateisysteme unter Linux

Linux unterstützt eine ganze Reihe von Dateisystemen. Dieses Kapitel gibt einen kurzen Überblick über die bekanntesten Dateisysteme unter Linux, wobei wir insbesondere auf deren Designkonzept und Vorzüge sowie deren Einsatzbereiche eingehen werden. Weiterhin werden einige Informationen zum „Large File Support“ unter Linux bereitgestellt.

18.1 Glossar 422
18.2 Die wichtigsten Dateisysteme unter Linux 422
18.3 Weitere unterstützte Dateisysteme 429
18.4 Large File Support unter Linux 430
18.5 Weitere Informationen 431

18.1 Glossar

Metadaten Die interne Datenstruktur eines Dateisystems, die eine geordnete Struktur und die Verfügbarkeit der Festplattendaten gewährleistet. Im Grunde genommen sind es die „Daten über die Daten". Nahezu jedes Dateisystem besitzt seine eigene Metadatenstruktur. Hierin liegt zum Teil auch der Grund für die unterschiedlichen Leistungsmerkmale der verschiedenen Dateisysteme. Es ist von äußerster Wichtigkeit, die Metadaten intakt zu halten, da andernfalls das gesamte Dateisystem zerstört werden könnte.

Inode Inodes enthalten alle möglichen Informationen über eine Datei, die Größe, die Anzahl der Links, Datum, Erstellungszeit, Änderungen, Zugriff sowie Zeiger (engl. *pointer*) auf die Festplattenblöcke, wo die Datei gespeichert ist.

Journal Im Zusammenhang mit einem Dateisystem ist ein Journal eine platteninterne Struktur mit einer Art Protokoll, in das der Dateisystemtreiber die zu ändernden (Meta-)daten des Dateisystems einträgt. „Journaling" verringert die Wiederherstellungszeit eines Linux-Systems enorm, da der Dateisystemtreiber keine umfassende Suche nach zerstörten Metadaten auf der gesamten Platte starten muss. Stattdessen werden die Journal-Einträge wieder eingespielt.

18.2 Die wichtigsten Dateisysteme unter Linux

Anders als noch vor zwei oder drei Jahren ist die Auswahl eines Dateisystems für Linux nicht mehr eine Angelegenheit von Sekunden (Ext2 oder ReiserFS?). Kernel ab der Version 2.4 bieten eine große Auswahl an Dateisystemen. Im Folgenden erhalten Sie einen groben Überblick über die grundlegende Funktionsweise dieser Dateisysteme und deren Vorteile.

Seien Sie sich immer bewusst, dass kein Dateisystem allen Applikationen gleichermaßen gerecht werden kann. Jedes Dateisystem hat seine ihm eigenen Stärken und Schwächen, die berücksichtigt werden müssen. Sogar das hochentwickeltste Dateisystem der Welt wird niemals ein vernünftiges Backupkonzept ersetzen.

Die Fachbegriffe „Datenintegrität" oder „Datenkonsistenz" beziehen sich in diesem Kapitel nicht auf die Konsistenz der Speicherdaten eines Benutzers (diejenigen Daten, die Ihre Applikation in ihre Dateien schreibt). Die

Konsistenz dieser Daten muss von der Applikation selbst gewährleistet werden.

Hinweis

Einrichtung von Dateisystemen

Soweit nicht explizit hier anders beschrieben, lassen sich alle Arbeiten zur Partitionierung und zum Anlegen und Bearbeiten von Dateisystemen bequem mit YaST erledigen.

Hinweis

18.2.1 Ext2

Die Ursprünge von Ext2 finden sich in der frühen Geschichte von Linux. Sein Vorgänger, das Extended File System, wurde im April 1992 implementiert und in Linux 0.96c integriert. Das Extended File System erfuhr eine Reihe von Änderungen und wurde für Jahre als Ext2 das bekannteste Dateisystem unter Linux. Mit dem Einzug der Journaling File Systeme und deren erstaunlich kurzen Wiederherstellungszeiten verlor Ext2 an Wichtigkeit.

Möglicherweise hilft Ihnen eine kurze Zusammenfassung der Stärken von Ext2 beim Verständnis für dessen Beliebtheit unter den Linux-Benutzern, die es teilweise noch heute als Dateisystem bevorzugen.

Stabilität Als wahrer „old-timer“, erfuhr Ext2 viele Verbesserungen und wurde ausführlich getestet. Daher wohl auch sein Ruf als „rock-solid“. Im Falle eines Systemausfalls, bei dem das Dateisystem nicht sauber ungemountet werden konnte, startet e2fsck eine Analyse der Dateisystemdaten. Metadaten werden in einen konsistenten Zustand gebracht und schwebende Dateien oder Datenblöcke werden in ein ausgewiesenes Verzeichnis geschrieben (genannt `lost+found/`). Im Gegensatz zu (den meisten) Journaling File Systemen analysiert e2fsck das gesamte Dateisystem und nicht nur die kürzlich veränderten Metadatenbits. Dies dauert bedeutend länger als die Überprüfung der Protokolldaten eines Journaling File Systems. Je nach Größe des Dateisystems kann dies eine halbe Stunde und mehr in Anspruch nehmen. Deshalb werden Sie Ext2 für keinen Server wählen, der hochverfügbar sein muss. Da Ext2 jedoch kein Journal pflegen muss und bedeutend weniger Speicher verbraucht, ist es manchmal schneller als andere Dateisysteme.

Leichtes Upgrade Basierend auf dem starken Fundament Ext2 konnte sich Ext3 zu einem gefeierten Dateisystem der nächsten Generation entwickeln. Seine Zuverlässigkeit und Stabilität wurden geschickt mit den Vorzügen eines Journaling File Systems verbunden.

18.2.2 Ext3

Ext3 wurde von Stephen Tweedie entworfen. Anders als alle anderen „next-generation" Dateisysteme, folgt Ext3 keinem komplett neuen Designprinzip. Es basiert auf Ext2. Diese beiden Dateisysteme sind sehr eng miteinander verwandt. Ein Ext3-Dateisystem kann leicht auf einem Ext2-Dateisystem aufgebaut werden. Der grundlegendste Unterschied zwischen Ext2 und Ext3 liegt darin, dass Ext3 Journaling unterstützt.

Zusammenfassend lassen sich für Ext3 drei Vorteile herausstellen:

Leichte und höchst zuverlässige Dateisystem-Upgrades von Ext2 Da Ext3 auf dem Ext2-Code basiert und sowohl sein platteneigenes Format als auch sein Metadatenformat teilt, sind Upgrades von Ext2 auf Ext3 sehr unkompliziert. Sie können sogar dann durchgeführt werden, wenn Ihre Ext2-Dateisysteme gemountet sind. Anders als beim Umstieg auf andere Journaling File Systeme, wie zum Beispiel ReiserFS, JFS, oder XFS, der sehr mühsam sein kann, (Sie müssen Sicherungskopien des gesamten Dateisystems erstellen und dieses anschließend von Grund auf neu erstellen), ist ein Umstieg auf Ext3 eine Angelegenheit von Minuten. Zugleich ist er sehr sicher, da die Wiederherstellung eines gesamten Dateisystems von Grund auf nicht immer fehlerlos vonstatten geht. Betrachtet man die Anzahl der vorhandenen Ext2-Systeme, die auf ein Upgrade auf ein Journaling File System warten, kann man sich leicht die Bedeutung von Ext3 für viele Systemadministratoren ausmalen. Ein Downgrade von Ext3 auf Ext2 ist genauso leicht wie das Upgrade. Führen Sie einfach einen sauberen Unmount des Ext3-Dateisystems durch und mounten Sie es als ein Ext2-Dateisystem.

Zuverlässigkeit und Performance Andere Journaling File Systeme folgen dem „metadata-only"-Journaling-Ansatz. Das heisst, Ihre Metadaten bleiben in einem konsistenten Zustand; dies kann jedoch nicht automatisch für die Dateisystemdaten selbst garantiert werden. Ext3 ist in der Lage, sich sowohl um die Metadaten als auch die Daten selbst zu kümmern. Wie eingehend sich Ext3 um Daten und

Metadaten kümmert, ist individuell einstellbar. Den höchsten Grad an Sicherheit (d.h. Datenintegrität) erreicht man durch den Start von Ext3 im `data=journal`-Modus; dies jedoch kann das System verlangsamen, da sowohl Metadaten als auch Daten selbst im Journal erfasst werden. Ein relativ neuer Ansatz besteht in der Verwendung des `data=ordered`-Modus, der sowohl die Daten- als auch die Metadatenintegrität gewährleistet, jedoch das Journaling nur für Metadaten verwendet. Der Dateisystemtreiber sammelt alle Datenblöcke, die zu einem Metadaten-Update gehören. Diese Blöcke werden als „transaction" gruppiert und werden auf die Platte geschrieben, bevor die Metadaten aktualisiert sind. Somit erreicht man Metadaten- und Datenkonsistenz ohne Leistungsverlust. Eine dritte Verwendungsart ist `data=writeback`. Hierbei können Daten in das Hauptdateisystem geschrieben werden, nachdem ihre Metadaten an das Journal übergeben wurden. Diese Option ist nach Meinung vieler aus Performancegründen die beste Einstellung. Jedoch kann es bei dieser Option passieren, dass alte Daten nach einem Absturz und einer Wiederherstellung in Dateien auftauchen, während die interne Dateisystemintegrität gewahrt wird. Sofern nicht anders angegeben, wird Ext3 mit der Standardeinstellung `data=ordered` gestartet.

Umwandeln eines Ext2-Dateisystems in Ext3

Anlegen des Journals: Rufen Sie `tune2fs -j` als Benutzer `root` auf. tune2fs legt das Ext3-Journal mit Standardparametern an. Möchten Sie selbst festlegen, wie groß und auf welchem Device das Journal angelegt werden soll, rufen Sie stattdessen `tune2fs -J` mit den beiden Parametern `size=` und `device=` auf. Mehr zu tune2fs entnehmen Sie der Manual-Page.

Festlegung des Dateisystemtyps in `/etc/fstab`
Damit das Ext3-Dateisystem auch als solches erkannt wird, öffnen Sie die Datei `/etc/fstab` und ändern Sie den Dateisystemtyp der betroffenen Partition von `ext2` in `ext3`. Nach dem nächsten Neustart des Systems ist Ihre Änderung wirksam.

`ext3` für das `root`-Verzeichnis verwenden
Wenn Sie Ihr `root` Dateisystem als `ext3` booten möchten, so ist es zusätzlich nötig, die Module `ext3` und `jbd` in die `initrd` zu integrieren. Tragen Sie die beiden Module hierzu in der Datei `/etc/sysconfig/kernel` bei den `INITRD_MODULES` zusätzlich ein, und rufen Sie den Befehl `mk_initrd` auf.

18.2.3 ReiserFS

Offiziell stand eine der Hauptfunktionen der Kernel-Version 2.4, ReiserFS seit der SUSE LINUX-Version 6.4 als Kernel-Patch für 2.2.x SuSE-Kernel zur Verfügung. ReiserFS stammt von Hans Reiser und dem Namesys-Entwicklungsteam. ReiserFS hat sich als mächtige Alternative zu Ext2 profiliert. Seine größten Vorteile sind bessere Festplattenspeicherverwaltung, bessere Plattenzugriffsleistung und schnellere Wiederherstellung nach Abstürzen. Einen kleinen Wermutstropfen gibt es dennoch: ReiserFS legt großen Wert auf die Metadaten, jedoch nicht auf die Daten selbst. Die nächsten Generationen von ReiserFS werden Data-Journaling beinhalten (sowohl Metadaten als auch tatsächliche Daten werden in das Journal geschrieben) sowie geordnete Schreibzugriffe (siehe `data=ordered` unter Ext3). Die Stärken von ReiserFS im Detail:

Bessere Festplattenspeicherverwaltung
: In ReiserFS werden alle Daten in einer Struktur namens B^*-balanced tree organisiert. Die Baumstruktur trägt zur besseren Festplattenspeicherverwaltung bei, da kleine Dateien direkt in den Blättern des B^*trees gespeichert werden können, statt sie an anderer Stelle zu speichern und einfach den Zeiger auf den tatsächlichen Ort zu verwalten. Zusätzlich dazu wird der Speicher nicht in Einheiten von 1 oder 4 kB zugewiesen, sondern in exakt der benötigten Einheit. Ein weiterer Vorteil liegt in der dynamischen Vergabe von Inodes. Dies verschafft dem Dateisystem eine größere Flexibilität gegenüber herkömmlichen Dateisystemen, wie zum Beispiel Ext2, wo die Inode-Dichte zum Zeitpunkt der Erstellung des Dateisystems angegeben werden muss.

Bessere Festplattenzugriffsleistung
: Bei kleinen Dateien werden Sie häufig bemerken können, dass sowohl die Dateidaten als auch die „stat_data“ (Inode)-Informationen nebeneinander gespeichert wurden. Ein einziger Festplattenzugriff reicht somit, um Sie mit allen benötigten Informationen zu versorgen.

Schnelle Wiederherstellung nach Abstürzen
: Durch den Einsatz eines Journals zur Nachverfolgung kürzlicher Metadatenänderungen reduziert sich die Dateisystemüberprüfung sogar für große Dateisysteme auf wenige Sekunden.

18.2.4 JFS

JFS, das „Journaling File System“ wurde von IBM für AIX entwickelt. Die erste Betaversion des JFS-Linux-Ports erreichte die Linux-Gemeinde im Sommer 2000. Version 1.0.0 wurde im Jahre 2001 herausgegeben. JFS ist auf die Bedürfnisse von Server-Umgebungen mit hohem Durchsatz zugeschnitten, da hierbei einzig die Performance zählt. Als volles 64-Bit-Dateisystem unterstützt JFS große Dateien und Partitionen (LFS oder *Large File Support*), was ein weiterer Pluspunkt für den Einsatz in Server-Umgebungen ist.

Ein genauerer Blick auf JFS zeigt, warum dieses Dateisystem möglicherweise eine gute Wahl für Ihren Linux-Server darstellt:

Effizientes Journaling JFS folgt wie ReiserFS einem „metadata only“-Ansatz. Anstelle einer ausführlichen Überprüfung werden lediglich Metadatenänderungen überprüft, die durch kürzliche Dateisystemaktivitäten hervorgerufen wurden. Dies spart enorm viel Zeit bei der Wiederherstellung. Zeitgleiche Aktivitäten, die mehrere Protokolleinträge erfordern, können in einem Gruppen-Commit zusammengefasst werden, wobei der Leistungsverlust des Dateisystems durch mehrfachen Schreibvorgang stark verringert wird.

Effiziente Verzeichnisverwaltung JFS hält an unterschiedlichen Verzeichnisstrukturen fest. Bei kleinen Verzeichnissen erlaubt es die direkte Speicherung des Verzeichnisinhaltes in seinem Inode. Für größere Verzeichnisse werden B^+trees verwendet, welche die Verzeichnisverwaltung erheblich erleichtern.

Bessere Speichernutzung durch dynamische Vergabe der Inodes Unter Ext2 müssen Sie die Inode-Dichte (von Verwaltungsinformationen belegter Speicher) vorab angeben. Dadurch wird die maximale Anzahl von Dateien oder Verzeichnissen Ihres Dateisystems limitiert. JFS erspart Ihnen diese Überlegungen — es weist Inode-Speicher dynamisch zu und stellt ihn bei Nichtbedarf wieder zur Verfügung.

18.2.5 XFS

Ursprünglich als Dateisystem für ihr IRIX-Betriebssystem gedacht, startete SGI die Entwicklung von XFS bereits in den frühen 90ern. Mit XFS sollte ein hochperformantes 64-Bit Journaling File System geschaffen werden, das den extremen Herausforderungen der heutigen Zeit gewachsen ist. XFS ist

gut geeignet für den Umgang mit großen Dateien und zeigt gute Leistungen auf High-end-Hardware. Jedoch weist sogar XFS eine Schwäche auf. Wie ReiserFS, legt XFS großen Wert auf Metadatenintegrität und weniger auf Datenintegrität.

Ein kurzer Blick auf die Schlüsselfunktionen von XFS erklärt, warum es sich möglicherweise als starke Konkurrenz zu anderen Journaling File Systemen in der High-end-Datenverarbeitung herausstellen könnte.

Hohe Skalierbarkeit durch den Einsatz von „Allocation groups“
Zum Erstellungszeitpunkt eines XFS-Dateisystems wird das dem Dateisystem zugrundeliegende Block-Device in acht oder mehr lineare Bereiche gleicher Größe unterteilt. Diese werden als „allocation groups“ bezeichnet. Jede Allocation group verwaltet Inodes und freien Speicher selbst. Allocation groups können praktisch als „Dateisysteme im Dateisystem“ betrachtet werden. Da Allocation groups relativ autonom sind, kann der Kernel gleichzeitig mehrere von ihnen adressieren. Hier liegt der Schlüssel zur hohen Skalierbarkeit von XFS. Das Konzept der autonomen Allocation groups kommt natürlicherweise den Anforderungen von Multiprozessorsystemen entgegen.

Hohe Performance durch effiziente Festplattenspeicherverwaltung
Freier Speicher und Inodes werden von B^+trees innerhalb der Allocation groups verwaltet. Der Einsatz von B^+trees trägt zu einem Großteil zur Leistung und Skalierbarkeit von XFS bei. Ein wahrhaft einzigartiges Funktionsmerkmal von XFS ist die „delayed allocation“. XFS verarbeitet die Speicherzuweisung (engl. *allocation*) durch Zweiteilung des Prozesses. Eine „schwebende“ Transaktion wird in RAM gespeichert und der entsprechende Speicherplatz reserviert. XFS entscheidet noch nicht, wo genau (d.h. in welchen Dateisystemblöcken) die Daten gespeichert werden. Diese Entscheidung wird bis zum letztmöglichen Moment hinausgezögert. Einige kurzlebige, temporäre Daten werden somit niemals auf Platte gespeichert, da sie zum Zeitpunkt der Entscheidung über ihren Speicherort durch XFS bereits obsolet sind. So XFS erhöht die Leistung und verringert die Dateisystemfragmentation. Da allerdings eine verzögerte Zuordnung weniger Schreibvorgänge als in anderen Dateisystemen zur Folge hat, ist es wahrscheinlich, dass der Datenverlust nach einem Absturz während eines Schreibvorgangs größer ist.

Preallocation zur Vermeidung von Dateisystemfragmentation
Vor dem Schreiben der Daten in das Dateisystem reserviert XFS den

benötigten Speicherplatz für eine Datei (engl. *preallocate*). Somit wird die Dateisystemfragmentation erheblich reduziert. Die Leistung wird erhöht, da die Dateiinhalte nicht über das gesamte Dateisystem verteilt werden.

18.3 Weitere unterstützte Dateisysteme

Tabelle 18.1 enthält weitere von Linux unterstützte Dateisysteme. Sie werden hauptsächlich unterstützt, um die Kompatibilität und den Datenaustausch zwischen unterschiedlichen Medien oder fremden Betriebssystemen sicherzustellen.

Tabelle 18.1: *Dateisystemarten unter Linux*

cramfs	*Compressed ROM file system*: ein komprimiertes Dateisystem mit Lesezugriff für ROMs.
hpfs	*High Performance File System*: das OS/2-Standarddateisystem — nur im Lesezugriffsmodus unterstützt.
iso9660	Standarddateisystem auf CD-ROMs.
ncpfs	Dateisystem zum Mounten von Novell-Volumes übers Netzwerk.
nfs	*Network File System*: Hierbei können Daten auf jedem beliebigen Rechner innerhalb eines Netzwerks gespeichert werden und der Zugriff kann über Netzwerk gewährt werden.
smbfs	*Server Message Block*: verwendet von Produkten wie zum Beispiel Windows für den Dateizugriff über ein Netzwerk.
sysv	verwendet unter SCO UNIX, Xenix und Coherent (kommerzielle UNIX-Systeme für PCs).
ufs	verwendet von BSD, SunOS und NeXTstep. Nur im Lesezugriffs-Modus unterstützt.
umsdos	*UNIX on MSDOS*: aufgesetzt auf einem normalen `fat`-Dateisystem. Erhält UNIX-Funktionalität (Rechte, Links, lange Dateinamen) durch die Erstellung spezieller Dateien.
vfat	*Virtual FAT*: Erweiterung des `fat`-Dateisystems (unterstützt lange Dateinamen).
ntfs	*Windows NT file system*: Lesezugriff.

18.4 Large File Support unter Linux

Ursprünglich unterstützte Linux Dateien bis zu einer maximalen Größe von 2 GB. Der zunehmende Einsatz von Linux zur Datenbankverwaltung, zur Verarbeitung von Audio- und Videodaten u.v.a.m. machten es nötig, Kernel und GNU C Library (*glibc*) für die Unterstützung größerer Dateien als 2 GB anzupassen. Es wurden neue Interfaces eingeführt, die von Applikationen genutzt werden können. Heutzutage bieten (fast) alle wichtigen Dateisysteme LFS-Unterstützung, die High-End-Datenverarbeitung erlaubt.

Tabelle 18.2 bietet einen Überblick über die derzeitigen Beschränkungen von Linux-Dateien und Dateisystemen.

Tabelle 18.2: *Maximale Größe von Dateisystemen (On-Disk Format)*

Dateisystem	**Max. Dateigröße**	**Max. Dateisystemgröße**
Ext2 oder Ext3 (1 kB Blockgröße)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 oder Ext3 (2 kB Blockgröße)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 oder Ext3 (4 kB Blockgröße)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 oder Ext3 (8 kB Blockgröße) (Systeme mit Pages von 8 kB (wie Alpha))	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS 3.5	2^{32} (4 GB)	2^{44} (16 TB)
ReiserFS 3.6 (unter Linux 2.4)	2^{60} (1 EB)	2^{44} (16 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
JFS (512 Bytes Blockgröße)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (4 kB Blockgröße)	2^{63} (8 EB)	2^{52} (4 PB)
NFSv2 (clientseitig)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (clientseitig)	2^{63} (8 EB)	2^{63} (8 EB)

Hinweis

Linux Kernel Limits

Die Tabelle beschreibt die Limits des on-disk Formats. Die maximale Größe einer Datei und eines Dateisystems, die vom Kernel korrekt verarbeitet werden kann, unterliegt unter Kernel 2.6 folgenden Beschränkungen:

- *Dateigröße:* Dateien können auf 32-bit Systemen nicht größer sein als 2 TB (2^{41} Byte).
- *Dateisystemgröße:* Dateisysteme können bis zu 2^{73} Byte groß sein. Dieses Limit schöpft (noch) keine aktuelle Hardware aus.

Hinweis

18.5 Weitere Informationen

Jedes der oben beschriebenen Dateisystemprojekte unterhält seine eigene Homepage, wo Sie Informationen aus Mailinglisten und weitere Dokumentation sowie FAQs erhalten.

- `http://e2fsprogs.sourceforge.net/ext2.html`
- `http://www.zipworld.com.au/~akpm/linux/ext3/`
- `http://www.namesys.com/`
- `http://oss.software.ibm.com/developerworks/opensource/jfs/`
- `oss.sgi.com/projects/xfs/`

Ein umfassendes mehrteiliges Tutorial zu Linux-Dateisystemen findet sich unter *IBM developerWorks*: `http://www-106.ibm.com/developerworks/library/l-fs.html`

Einen Vergleich der verschiedenen Journaling File Systeme unter Linux befindet sich im Beitrag von Juan I. Santos Florido unter *Linuxgazette*: `http://www.linuxgazette.com/issue55/florido.html`

Eine ausführliche Arbeit zu LFS unter Linux erhält man auf Andreas Jaegers LFS-Seiten: `http://www.suse.de/~aj/linux_lfs.html`

Hochverfügbarkeit unter Linux

Dieses Kapitel stellt in einem Kurzüberblick wesentliche Konzepte und Werkzeuge aus dem Bereich der Hochverfügbarkeit unter Linux vor. Zusätzlich erhalten Sie zu allen vorgestellten Themen weiterführende Literaturhinweise.

19.1 Wichtige Begriffe 434
19.2 Ein minimales Beispielszenario 435
19.3 Komponenten einer Hochverfügbarkeitslösung . . 436
19.4 Die Softwareseite von Hochverfügbarkeit 438
19.5 Clustering 439
19.6 Weitere Informationen 440

Hochverfügbarkeit beschreibt Systeme, die bestimmte Störungen – insbesondere Ausfälle von einzelnen Rechnern – maskieren können, um dem Benutzer den Dienst nach einer kurzen Ausfallzeit wieder anzubieten. Hierzu werden Hard- und Software sorgfältig aufeinander abgestimmt und redundant ausgelegt, um im Falle einer Störung automatisch auf die andere Komponente umschalten zu können. Hochverfügbarkeit unterscheidet sich von „fehlertolerant“ dadurch, dass für diese kurze Phase des Umschaltens der Dienst temporär nicht verfügbar ist, was sich in Verzögerungen oder kurzen Verbindungsabbrüchen zeigen kann.

Von hochverfügbaren Systemen spricht man insbesondere, wenn die Gesamtverfügbarkeit des Dienstes zwischen 99.999% und 99.99999% liegt; dies entspricht auf ein Jahr hochgerechnet zwischen 5 Minuten und 3 Sekunden. Besonders wichtig ist dabei jedoch nicht nur die Soft- und Hardwareseite, sondern an erster Stelle die durchdachte Systemadministration mit dokumentierten und nachvollziehbaren Prozessen, um Fehler zu minimieren. Es handelt sich hierbei in jedem Fall um eine Risiko/Kosten-Abwägung; je nach Anwendungsszenario können unterschiedliche Anforderungen und Lösungen angebracht sein. Ihr Novell Partner berät Sie gerne.

19.1 Wichtige Begriffe

Vorab einige wichtige Begriffe, die im Zusammenhang mit Hochverfügbarkeit immer wieder auftauchen:

SPOF *Single Point of Failure*: Komponente eines Systems, bei deren Ausfall die Funktionalität des Gesamtsystems beeinträchtig wird.

Failover Eine andere gleichartige Systemkomponente übernimmt automatisch die Funktion einer ausgefallenen Komponente.

Cold Standby Die Ersatzhardware steht „kalt“ bereit. Die Übernahme muss manuell erfolgen, sodass der Ausfall dementsprechend auch deutlich spürbar ist.

Warm Standby Das Backupsystem läuft im Hintergrund mit, sodass die Übernahme automatisch erfolgen kann. Die Daten auf beiden Systemen werden automatisch synchronisiert. Die Übernahme (Failover) spürt der Benutzer ähnllich wie einen sehr schnellen automatischen Reboot des Dienstes. Allerdings kann die aktuelle Transaktion möglicherweise abgebrochen werden, da die Daten vor dem Ausfall nicht mehr synchronisiert werden konnten.

Hot Standby Beide Systeme laufen ständig parallel – Daten auf beiden Systemen sind hundertprozentig synchron. Der Benutzer spürt nichts von eventuellen Ausfällen. Meist ist diese Stufe nicht ohne eine entsprechende Modifikation des Clients zu erreichen. Um beide Systeme 100% synchron zu betreiben, müssen auch die Verbindungen zum Client 100% gespiegelt werden. Dafür braucht man normalerweise Clients, die Verbindungen zu zwei oder mehr Servern gleichzeitig halten und mit allen reden. Das kann beispielsweise ein normaler Webbrowser nicht.

Load Balancing Lastenverteilung innerhalb eines Clusters von Rechnern. Zum Einsatz kommt *Load Balancing* zum Beispiel in einem LVS-Szenario (*Linux Virtual Server*) (siehe Abschnitt 19.5.2 auf Seite 439).

STONITH *Shot the other node in the head*: Spezielle Hardware/Software, die sicherstellt, dass ein defekter Knoten innerhalb eines Clusters keine Schreibzugriffe auf verteilte Medien durchführt und die Datenkonsistenz im gesamten Cluster gefährdet. Dazu wird das System schlicht vom Stromnetz getrennt.

19.2 Ein minimales Beispielszenario

Die Vorgänge innerhalb eines 2-Node-Clusters beim Ausfall eines Knotens und die verschiedenen Arten des Standby-Systems, das bei Bedarf übernimmt, werden im Folgenden skizziert (siehe Abbildung 19.1 auf der nächsten Seite).

Die beiden Server (Primary und Backup) stehen beide mit einem SAN (Storage Area Network) in Verbindung. Je nach Betriebsart greift nur der jeweils aktive Knoten hierauf auch zu. Untereinander kommunizieren beide in der Form, dass sie sich regelmäßig „Lebenszeichen“ (heartbeat) senden. Die Kommunikationswege (oder *hearbeat links*) sind ebenfalls redundant ausgelegt, indem voneinander unabhängige Wege über unterschiedliche Netzwerkkarten und Kabelwege genutzt werden. Fällt einer der Links aus, melden seine Backups weiterhin korrekt, dass der entsprechende Server „am Leben“ ist. Bleiben die Lebenszeichen des Hauptsystems aus, wird das Standby-System aktiviert, übernimmt die Dienste des ausgefallenen Partners und nimmt ihn komplett vom Netz (siehe oben *STONITH*).

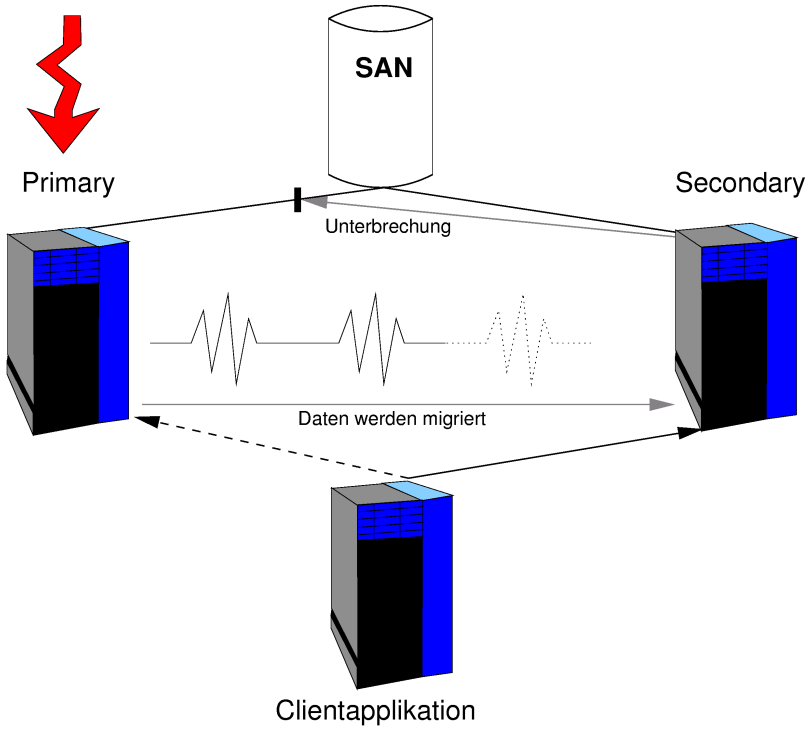

Abbildung 19.1: *Ein einfaches Hochverfügbarkeitscluster*

19.3 Komponenten einer Hochverfügbarkeitslösung

Eine Hochverfügbarkeitslösung setzt sich aus mehreren verschiedenen Komponenten zusammen:

Generelle Infrastruktur Allgemein muss beim Konzipieren einer hochverfügbaren Lösung bedacht werden, dass auch die Aufstellung aller wichtiger Server an einem einzigen Ort ein potentieller *SPOF* sein kann, wenn dieser Standort von (Umwelt)-Katastrophen oder Stromausfällen betroffen sein sollte. Ausserdem muss auf die „Umweltbedingungen“ der Server geachtet werden – (redundante) Klimaanlagen sind unerlässlich.

Hardware Ohne größtmögliche Ausfallsicherheit auf Hardwarebene verhilft auch die ausgefeilteste Softwarelösung nicht zum hochverfügbaren System. Die wichtigsten Hardwarekomponenten, die bedacht und möglichst redundant ausgelegt werden sollten, sind:

Stromversorgung Nach Möglichkeit sichern Sie Ihre Server über eine USV (unterbrechungsfreie Stromversorgung) ab, um sicherzustellen, dass ein kurzer Spannungsabfall überbrückt werden kann und bei einem längeren Ausfall ein sauberes Herunterfahren der Systeme möglich ist. Selbstverständlich sollte auch die Stromversorgung redundant ausgelegt werden.

Netzwerkschnittstellen Stellen Sie sicher, dass jedes Ihrer Systeme mehrere Netzwerkschnittstellen besitzt. Fällt eine aus, muss automatisch eine der anderen Adresse und Aufgabe der ausgefallenen Komponente übernehmen. Die Redundanz bezieht sich hier ausdrücklich auf beide Richtungen von Schnittstellen. Es schadet nicht, sowohl für die interne Schnittstelle als auch die externe jeweils eine aktive und ein Backup einzuplanen.

Festplatten Versehen Sie Ihre Systeme mit mehreren Festplatten und legen Sie die Datensicherung (z.B. mittels RAID oder drbd) so aus, dass beim Verlust einer dieser Platten die anderen stets den intakten Datensatz enthalten. Eine defekte Platte muss ohne Halt des Systems gegen eine neue Platte auswechselbar sein.

Anwendungen Alle wichtigen Dienste und Anwendungen, die Ihre Systeme nach aussen präsentiert, müssen so ausgelegt sein, dass sie einen Neustart nicht behindern. Gibt eine Anwendung nach einem Crash ihre Lockdateien nicht frei, verhindern diese den Neustart des entsprechenden Prozesses. Damit ist diese Anwendung nicht für eine Hochverfügbarkeitsumgebung geeignet. Idealerweise wird die „Gesundheit" bestimmter Anwendungen, von Betriebssystemprozessen und der Netzwerkverbindungen mit einem geeigneten Monitoring-Tool überwacht.

Daten Alle wichtigen Daten müssen nach Ausfall eines Systems dem übernehmenden System vollständig und intakt zur Verfügung stehen. Diese Art der Hochverfügbarkeit erreicht man, indem Daten verteilt über mehrere Systeme oder Festplatten gespeichert werden. Dazu werden die Inhalte einer Platte regelmäßig auf eine (oder mehrere) weitere gespiegelt, die bei einem Ausfall mit dem intakten Datensatz übernehmen kann. Damit ein Dateisystem nach Systemabsturz in konsistentem Zustand wieder hochkommt, verwenden Sie ein Journaling Filesystem.

Netzwerk Legen Sie alle Netzwerkinfrastrukur von der Router/Switch-Infrastruktur bis hinunter zum simplen Netzwerkkabel redundant aus.

19.4 Die Softwareseite von Hochverfügbarkeit

In den folgenden Abschnitten werden die wichtigsten Softwareaspekte von hochverfügbaren Lösungen vorgestellt:

19.4.1 heartbeat

heartbeat ist ein Paket, das zur Überwachung aller im Cluster befindlichen Knoten eingesetzt wird. heartbeat tauscht auf den Netzwerkschnittstellen der Clustermitglieder „Herzschläge“ (engl. *heartbeat*) aus, um zu ermitteln, welche Knoten im Cluster aktiv sind. Fällt ein Knoten aus, unterbleibt sein Signal. heartbeat sorgt in diesem Fall dafür, dass ein anderer Knoten dessen Aufgaben und Identität übernimmt und die Übernahme im Netz bekannt macht. So bleibt das Cluster konsistent. Derzeit ist die Failover-Funktion von heartbeat auf zwei Knoten beschränkt.

19.4.2 RAID

RAID (engl. *Redundant Array of Independent Disks*) vereint mehrere Festplattenpartitionen zu einer großen *virtuellen* Festplatte. Mittels RAID lassen sich Performance und Datensicherheit Ihres Systems optimieren. Die RAID-Level 1 und 5 bieten eine Absicherung gegen den Ausfall einer Platte, da die Daten gleichzeitig auf mehre Platten geschrieben werden. So ist nach Ausfall einer Platte stets der komplette Datensatz auf einer anderen Platte im System vorhanden. Mehr Informationen zu RAID unter SUSE LINUX erhalten Sie in Abschnitt 3.11 auf Seite 160.

19.4.3 rsync

Zur Synchronisation großer Datenmengen zwischen einem Server und seinem Backup bietet sich rsync an. rsync verfügt über ausgefeilte Mechanismen, um ausschließlich Änderungen an Dateien zu übertragen. Dies

betrifft nicht nur Textdateien, sondern auch binäre Dateien. Um die Unterschiede zwischen Dateien zu erkennen, teilt rsync die Dateien in Blöcke auf, und berechnet Prüfsummen zu diesen Blöcken. Mehr Informationen zu rsync erhalten Sie in Abschnitt 23.6 auf Seite 625.

19.4.4 DRBD

Distributed Replicated Block Device (drbd) ermöglicht die Spiegelung (RAID1) von Partitionen/Logical Volumes (Datenbereichen) über ein normales Netzwerk auf TCP/IP-Basis. Jeweils ein Knoten hat eine bestimmte drbd Resource „aktiv“, und jegliche Änderungen werden transaktionssicher auf den Mirror gespiegelt.

Gegenüber dem RAID1 von lokalen Platten bietet drbd zusätzliche Features, um die Resynchronisationszeit nach einer kurzzeitigen Trennung der beiden Knoten zu minimieren, und nach diversen Störungen robust zu ermitteln, welche Seite die aktuellen und konsistenten Daten zur Verfügung stellt.

19.5 Clustering

19.5.1 Cluster Alias

Der Cluster Alias ist eine Technologie, bei der mehrere Knoten eine gemeinsame IP-Adresse konfiguriert haben und auch auf dieser Adresse TCP/IP-Verbindungen aufbauen können. Eingehende TCP/IP-Verbindungen werden dabei automatisch verteilt.

Im Gegensatz zum Linux Virtual Server wird kein dedizierter Load Balancer benötigt. Allerdings ist der Cluster Alias durch die Art der Implementierung bei einer größeren Anzahl von Knoten weniger effizient: Beim Cluster Alias werden alle IP-Pakete an alle Knoten verteilt, die sich dann jeweils die für sie bestimmten herausfiltern, wohingegen beim LVS diese Entscheidung nur einmalig vom Load Balancer getroffen wird. Nähere Informationen zur Konfiguration dieses Features entnehmen Sie bitte der Manualpage von iptables.

19.5.2 Linux Virtual Server

Linux Virtual Server baut auf einem realen Cluster mehrerer Server auf, die über einen Load Balancer zur Lastverteilung auf die einzelnen Clustermitglieder miteinander verbunden sind. Nach aussen hin präsentiert sich solch

ein Cluster lediglich als ein einzelner virtueller Server. Selbstverständlich sollte der Load Balancer ebenfalls redundant ausgelegt sein und per heartbeat abgesichert werden. Ziel einer LVS-Konfiguration ist die bestmögliche Ausnutzung der verhandenen Ressourcen und die gute Skalierbarkeit. Um die „Gesundheit" der einzelnen realen Server zu überwachen, wird in diesen Szenarien der heartbeat-ldirectord Daemon eingesetzt.

19.5.3 High-Availability Cluster

Ein High-Availability Cluster ist so konzipiert, dass es jederzeit alle angebotenen Dienste trotz Hard- oder Softwareausfall anbieten kann. Wenn ein Knoten des Clusters ausfällt, übernimmt sofort ein anderer. Der übernehmende Knoten (*secondary*) ist ein Spiegelbild des ausgefallenen Knotens (*primary*) und nimmt beim Failover sogar die Identität des ausgefallenen Knotens an, womit die Clusterumgebung nach aussen hin konsistent bleibt.

19.6 Weitere Informationen

19.6.1 Hochverfügbarkeit (HA) allgemein und heartbeat

Erste Anlaufstelle zum Thema Hochverfügbarkeit unter Linux ist die Homepage des *Linux-HA* Projekts (`http://linux-ha.org`). Hier finden Sie eine Fülle weiterführender Tipps und Links auf Dokumentationen, Erfahrungsberichte und Szenarien.

Gedruckte Information zum Thema Hochverfügbarkeit finden Sie in dem Buch *Blueprints in High Availability*:

Marcus, Evan & Stern, Hal: *Blueprints in High Availability*. John Wiley & Sons Inc., 2000. - (ISBN 0-471-35601-8)

► **zSeries, S/390**
Für Linux auf IBM S/390 und zSeries existiert ein sehr ausführliches Redpaper mit zahlreichen Beispielszenarien und -konfigurationen unter: `http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp0220.html`. ◄

Ein Wiki zum Thema HA und hearbeat: `http://wiki.trick.ca/linux-ha/PressRoom` und `http://wiki.trick.ca/linux-ha/HeartbeatTutorials`

19.6.2 DRBD

Die Homepage des DRBD-Projekts: `http://www.drbd.org/`

Ein Artikel des englischsprachigen Linux-Magazins zum Thema:`http://www.linux-mag.com/2003-11/drbd_01.html`

19.6.3 RAID

Eine umfangreiche Linksammlung zum RAID-Themenkomplex: `http://linas.org/linux/raid.html`

19.6.4 Clustering

Zum Thema Clustering bietet die Homepage des *Linux Clustering Information Center* weitere Informationen: `http://www.lcic.org/`

Die Homepage des *Linux Virtual Server* Projekts: `http://www.linuxvirtualserver.org/`

Zum *Oracle Cluster File System* finden Sie Informationen auf der Homepage des Projekts unter `http://oss.oracle.com/projects/ocfs/`, sowie ausführliche Dokumentationen unter: `http://oss.oracle.com/projects/ocfs/documentation/`.

PAM – Pluggable Authentication Modules

PAM (engl. *Pluggable Authentication Modules*) wird unter Linux verwendet, um bei der Authentifizierung zwischen Benutzer und Anwendung zu vermitteln. PAM-Module stehen zentral zur Verfügung und können von jeder Applikation aufgerufen werden. Wie diese modulare Authentifizierung konfiguriert wird und wie sie arbeitet, ist Inhalt dieses Kapitels.

20.1 Aufbau einer PAM-Konfigurationsdatei 444
20.2 Die PAM-Konfiguration von sshd 446
20.3 Konfiguration der PAM-Module 447
20.4 Weitere Informationen 450

Systemadministratoren und Entwickler möchten den Zugriff auf bestimmte Systembereiche oder die Nutzung bestimmter Funktionaliäten einer Anwendung beschränken. Ohne PAM würde dies bedeuten, dass alle Anwendungen immer wieder an neue Authentifizierungsschemen (z.B. LDAP oder Samba) angepasst werden müssten. Dieses Vorgehen ist zeitraubend und fehleranfällig. Löst man hingegen die Authentifizierung von der Anwendung und delegiert sie an zentrale Module, entfallen diese Nachteile. Soll ein neues Authentifizierungsschema angewandt werden, muss lediglich ein PAM-Modul angepasst/entwickelt werden, auf das die Anwendung zurückgreifen kann.

Für jedes Programm, das PAM nutzt, liegt eine eigene Konfigurationsdatei unter `/etc/pam.d/<dienst>/`. In dieser Datei ist festgelegt, welche PAM-Module zur Benutzerauthentifizierung verwendet werden sollen. Globale Konfigurationsdateien der meisten PAM-Module unter `/etc/security/` legen das genaue Verhalten dieser Module fest (Beispiele: `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf`, `time.conf` usw. ...). Eine Applikation, die ein PAM-Modul nutzt, ruft einen bestimmten Satz an PAM-Funktionen auf, die die Informationen aus den verschiedenen Konfigurationsdateien verarbeiten und das Ergebnis an die aufrufende Anwendung weiterleiten.

20.1 Aufbau einer PAM-Konfigurationsdatei

Eine Zeile einer PAM-Konfigurationsdatei baut sich aus maximal vier Spalten auf:

```
<Modultyp> <Kontroll-Flag> <Modulpfad> <Optionen>
```

PAM-Module werden stapelweise abgearbeitet. Die verschiedenen Module haben unterschiedliche Aufgaben. Ein Modul übernimmt die Passwortprüfung, ein anderes prüft, von woher der Zugriff erfolgt und ein weiteres fragt benutzerspezifische Systemeinstellungen ab.

PAM kennt vier verschiedene Typen von Modulen:

`auth` Module dieses Typs dienen der Überprüfung, ob der Benutzer authentisch ist. Diese Überprüfung geschieht traditionell durch Passwortabfrage, kann aber auch per Chipkarte oder über Prüfung eines biometrischen Merkmals (Fingerabdruck, Irisscan) erfolgen.

`account` Module dieses Typs überprüfen, ob der Benutzer authorisiert ist, den angefragten Dienst überhaupt zu benutzen. So sollte sich zum Beispiel niemand mit abgelaufenem Account auf einem System einloggen können.

`password` Module dieses Typs dienen der Änderung des Authentifizierungsmerkmals. Dies ist in den meisten Fällen ein Passwort.

`session` Module dieses Typs sind zur Verwaltung und Konfiguration von Benutzer-Sessions gedacht. Diese Module werden vor und nach der Authentifizierung gestartet, um Loginversuche zu protokollieren und dem Benutzer seine eigene Umgebung zuzuweisen (Mailzugang, Homeverzeichnis, Systemlimits usw.)

Die zweite Spalte enthält die Kontroll-Flags, mit denen die gewünschten Module aufgerufen werden:

`required` Das Modul muss erfolgreich abgearbeitet werden, damit die Authentifizierung fortschreiten kann. Bei Fehlschlagen eines `required` Moduls werden noch alle anderen Module dieses Typs abgearbeitet, bevor der Benutzer eine Meldung über das Fehlschlagen seines Authentifizierungsversuchs erhält.

`requisite` Diese Module müssen ebenso wie die `required` Module erfolgreich abgearbeitet werden. Bei einem Fehlschlag erhält der Benutzer unmittelbares Feedback und es werden keine weiteren Module mehr abgearbeitet. Im Erfolgsfall werden weitere Module genau wie bei `required` abgearbeitet. Dieses Flag kann als ein einfacher Filter eingesetzt werden, um bestimmte Bedingungen abzufragen, die für eine korrekte Authentifizierung notwendig sind.

`sufficient` Wird ein Modul dieses Typs erfolgreich abgearbeitet, erhält das aufrufende Programm sofort eine Erfolgsmeldung und es werden keine weiteren Module mehr abgearbeitet, wenn kein voranstehendes `required`-Modul fehlgeschlagen ist. Schlägt ein `sufficient`-Modul fehl, hat dies keine Folgen und die folgenden Module werden der Reihe nach weiter abgearbeitet.

`optional` Erfolg oder Fehlschlag hat keinerlei Auswirkung. Diese Eigenschaft wird zum Beispiel bei Modulen verwendet, die anzeigen sollen, ob ein Benutzer E-Mail erhalten hat, aber keine weiteren Auswirkungen haben.

Der Modulpfad wird nicht explizit angegeben, wenn die Module im Standardverzeichnis `/lib/security/` (bzw. unter `/lib64/security/` bei allen von SUSE LINUX unterstützten 64-bit Plattformen) zu finden sind. Als vierter Eintrag kann einem Modul noch eine Option wie zum Beispiel `debug` (Debugmodus) oder `nullok` (leere Passwörter sind erlaubt) übergeben werden.

20.2 Die PAM-Konfiguration von sshd

Nachdem der Theorie zur PAM-Konfiguration hier nun ein praktisches Beispiel, die sshd PAM-Konfiguration:

Beispiel 20.1: *PAM-Konfiguration für sshd*

```
#%PAM-1.0
auth required   pam_unix2.so # set_secrpc
auth required   pam_nologin.so
auth required   pam_env.so
account required        pam_unix2.so
account required        pam_nologin.so
password required       pam_pwcheck.so
password required       pam_unix2.so    use_first_pass use_authtok
session required        pam_unix2.so    none     # trace or debug
session required        pam_limits.so
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

Zuerst ruft sshd die drei Module vom Typ `auth` auf. Das erste Modul, `pam_unix2` prüft Login und Passwort des Benutzers anhand von `/etc/passwd` und `/etc/shadow`. Das nächste Modul (`pam_nologin`) prüft, ob die Datei `/etc/nologin` existiert. Ist dies der Fall, hat ausser `root` kein anderer Benutzer Zugang. Das dritte Modul `pam_env` liest die Datei `/etc/security/pam_env.conf` ein und setzt die dort spezifizierten Umgebungsvariablen. Hier lässt sich beispielsweise die `DISPLAY`-Variable auf den richtigen Wert setzen, da `pam_env` Informationen darüber erhält, von wo sich ein Benutzer einzuloggen versucht. Der „Stapel“ (engl. *stack*) der `auth`-Module wird abgearbeitet, bevor der ssh-Daemon eine Rückmeldung darüber bekommt, ob die Anmeldung erfolgreich war oder nicht. Alle Module tragen hier den Kontroll-Flag `required` und müssen sämtlich erfolgreich abgearbeitet worden sein, bevor die Erfolgsmeldung an sshd

abgesetzt wird. Schlägt eines dieser Module fehl, bewirkt das zwar, dass das Endergebnis negativ ist, aber sshd erfährt davon erst, wenn alle Module dieses Typs abgearbeitet wurden.

Im nächsten Modulstapel werden alle Module vom Typ `account` abgearbeitet, die die Überprüfung übernehmen, ob der betreffende Benutzer überhaupt berechtigt ist, den angefragten Dienst auszuführen. Hierzu müssen wiederum die Module `pam_unix2` und `pam_nologin` erfolgreich abgearbeitet werden (`required`). Meldet `pam_unix2` zurück, dass dieser Benutzer existiert, und hat `pam_nologin` sichergestellt, dass er nicht vom Login ausgeschlossen ist, wird eine Erfolgsmeldung an sshd abgesetzt und die nächste Modulgruppe in Angriff genommen.

Die folgenden beiden Module gehören zum Typ `password` und müssen ebenfalls erfolgreich abgearbeitet werden (Kontroll-Flag: `required`), wenn die Anwendung das Authentifizierungstoken ändert. Um ein Passwort oder ein anderes Authentifizierungstoken zu ändern, muss es auf seine Sicherheit geprüft werden. Das PAM-Modul `pam_pwcheck` sorgt dafür, dass das Passwort von der CrackLib-Bibliothek auf seine Sicherheit hin überprüft wird und den Benutzer ggf. warnt, sollte er ein unsicheres (zu kurzes, zu einfaches) Passwort wählen. Das schon bekannte `pam_unix2`-Modul übernimmt die alten und neuen Passwörter von `pam_pwcheck`. So muss der Benutzer sich nicht erneut authentifizieren. Ausserdem wird so ein Umgehen der Checks von `pam_pwcheck` verhindert. Die Module vom Typ `password` sollten immer dann aufgerufen werden, wenn die vorangestellten Module für `account` oder `auth` ein abgelaufenes Passwort bemängeln.

Zum Abschluss werden die Module vom Typ `session` aufgerufen, um die Session den Vorgaben für diesen Benutzer entsprechend zu konfigurieren. Das `pam_unix2`-Modul wird hier zwar erneut aufgerufen, mit der Option `none` hat dieser Aufruf aber keinerlei praktische Auswirkungen. Das Modul `pam_limits` liest die Datei `/etc/security/limits.conf` ein, in der eventuelle Limits für die Benutzung von Systemressourcen festgelegt werden können. Loggt der Benutzer sich wieder aus, werden die `session`-Module erneut aufgerufen.

20.3 Konfiguration der PAM-Module

Die Arbeitsweise mancher PAM-Module ist konfigurierbar. Die dazugehörigen Konfigurationsdateien befinden sich unter `/etc/security/`. Dieser Abschnitt geht kurz auf die im sshd Beispiel verwendeten Dateien ein.

Dies sind `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` und `limits.conf`.

20.3.1 pam_unix2.conf

Für die traditionelle Passwort-Authentifizierung wird das PAM Modul `pam_unix2` verwendet. Es kann seine Daten aus `/etc/passwd`, `/etc/shadow`, über NIS-Maps, über NIS+-Tabellen oder über eine LDAP-Datenbank beziehen. Diesem Modul können seine Konfigurationsoptionen entweder individuell in der PAM-Konfiguration der Anwendung übergeben werden oder global in `/etc/security/pam_unix2.conf`.

Im einfachsten Fall sieht diese Datei folgendermaßen aus:

Beispiel 20.2: *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

Die Option `nullok` für die `auth` und `password` Modultypen besagt, dass leere Passwörter für diese Art des Accounts zulässig sind. Der Benutzer hat das Recht, die Passwörter zu ändern. Mittels der Option `none` für den `session` Typ wird festgelegt, dass für diesen Modultyp keine Meldungen geloggt werden (Standardeinstellung). Weitere Konfigurationsoptionen können Sie den Kommentaren in dieser Datei oder der Manualpage von pam_unix2 entnehmen.

20.3.2 pam_env.conf

Diese Datei kann verwendet werden, um Benutzern nach Aufruf des `pam_env`-Moduls eine standardisierte Umgebung vorzugeben. Die Syntax zum Setzen der Umgebungsvariablen ist:

```
VARIABLE  [DEFAULT=[wert]]  [OVERRIDE=[wert]]
```

`VARIABLE` Bezeichner der Umgebungsvariable, die gesetzt werden soll

`[DEFAULT=[wert]]` Standardwert, den der Administrator als Standard vorgeben möchte

[OVERRIDE=[wert]] Werte, die `pam_env` ermitteln und einsetzen kann, um den Standardwert zu überschreiben

Ein berühmtes Beispiel, wie `pam_env` eingesetzt werden kann, ist die Anpassung der DISPLAY-Variablen für Login übers Netz:

Beispiel 20.3: *pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

Die erste Zeile setzt den Wert der Variablen `REMOTEHOST` auf `localhost`, so `pam_env` nicht einen anderen Wert ermitteln kann und zurückgibt. Die Variable `DISPLAY` nutzt den Variablenwert von `REMOTEHOST`. Mehr Informationen erhalten Sie in den Kommentaren der `/etc/security/pam_env.conf`-Datei.

20.3.3 pam_pwcheck.conf

Aus dieser Datei holt sich das Modul `pam_pwcheck` die Optionen für alle Module vom Typ `password`. Die hier gespeicherte Einstellung wird vor derjenigen in der PAM-Konfiguration der Anwendung gelesen. Wenn für die Anwendung keine individuelle Einstellung vorgenommen wurde, wird die globale Einstellung verwendet. Ein Beispiel ist die folgende Konfiguration:

Beispiel 20.4: *pam_pwcheck.conf*

```
password:    nullok blowfish use_cracklib
```

`pam_pwcheck` wird angewiesen, leere Passwörter und das Ändern von Passwörtern zu verwenden, den Blowfish-Algorithmus für die Verschlüsselung zu verwenden und die Passwortüberprüfung durch die CrackLib-Bibliothek vorzunehmen. Mehr Optionen finden Sie in der Datei `/etc/security/pam_pwcheck.conf`.

20.3.4 limits.conf

Das Modul `pam_limits` liest die Systemlimits für bestimmte Benutzer oder Gruppen aus der Datei `limits.conf` aus. Theoretisch besteht hier die Möglichkeit, harte (keine Überschreitung möglich) und weiche (temporäre Überschreitung erlaubt) Limits auf Systemressourcen zu setzen. Die Syntax und möglichen Optionen entnehmen Sie der Datei selbst.

20.4 Weitere Informationen

Auf Ihrem installierten System finden Sie im Verzeichnis `/usr/share/doc/packages/pam/` folgende Dokumentationen:

READMEs Auf oberster Ebene in diesem Verzeichnis finden Sie einige allgemeine READMEs. Im Unterverzeichnis `modules/` finden Sie die READMEs zu den verfügbaren PAM-Modulen.

The Linux-PAM System Administrators' Guide
Alles Wissenswerte zum PAM, das ein Systemadministrator wissen muss. Hier werden Themen etwa von der Syntax einer PAM-Konfigurationsdatei bis hin zu Sicherheitsaspekten behandelt. Diese Information ist in den Formaten PDF, HTML oder Text verfügbar.

The Linux-PAM Module Writers' Manual
Hier sind die Informationen gebündelt, die ein Entwickler benötigt, um standardkonforme PAM-Module zu schreiben. Diese Information ist in den Formaten PDF, HTML oder Text verfügbar.

The Linux-PAM Application Developers' Guide
Dieses Dokument enthält alles, was ein Anwendungsentwickler wissen muss, wenn er die PAM-Bibliotheken nutzen möchte. Diese Information ist in den Formaten PDF, HTML oder Text verfügbar.

Eine grundsätzliche Einführung in PAM von Thorsten Kukuk ist unter `http://www.suse.de/~kukuk/pam/PAM_lt2000/siframes.htm` verfügbar. Unter `http://www.suse.de/~kukuk/pam/` finden sich weitere Informationen zu bestimmten PAM-Modulen, die von ihm für SUSE LINUX entwickelt wurden.

Teil III

Dienste

Grundlagen der Vernetzung

Linux, ein wahres Kind des Internets, bietet Ihnen alle Voraussetzungen und notwendigen Netzwerktools zur Einbindung in diverse Netzwerkstrukturen. Im folgenden erhalten Sie eine Einführung in das normalerweise von Linux verwendete Protokoll TCP/IP, dessen Dienstleistungen und auch besonderen Eigenschaften. Anschließend zeigen wir Ihnen die Einrichtung eines Netzwerkzugangs mit einer Netzwerkkarte unter SUSE LINUX mit Hilfe von YaST. Es werden die zentralen Konfigurationsdateien besprochen und einige der wichtigsten Tools aufgeführt. Da die Konfiguration eines Netzwerks beliebig komplex sein kann, werden in diesem Kapitel nur die grundlegenden Mechanismen dargestellt.

21.1 TCP/IP – Das von Linux verwendete Protokoll . . 454
21.2 IPv6 – Internet der nächsten Generation 463
21.3 Manuelle Netzwerkkonfiguration 472
21.4 Die Einbindung ins Netzwerk 481
21.5 Routing unter SuSE Linux 497
21.6 SLP — Dienste im Netz vermitteln 498
21.7 DNS – Domain Name System 502
21.8 LDAP – Ein Verzeichnisdienst 521
21.9 NIS – Network Information Service 553
21.10 NFS – verteilte Dateisysteme 557
21.11 DHCP 563
21.12 Zeitsynchronisation mit xntp 577

21.1 TCP/IP – Das von Linux verwendete Protokoll

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Genau genommen handelt es sich um eine Protokollfamilie, die ganz unterschiedliche Dienstleistungen bietet. TCP/IP wurde aus einer militärischen Anwendung heraus entwickelt und in der heute verwendeten Form ca. 1981 in einem so genannten RFC festgelegt. Bei RFC (engl. *Request for comments*) handelt es sich um Dokumente, die die verschiedenen Internetprotokolle und die Vorgehensweise bei der Implementierung des Betriebssystems und von Applikationen beschreiben. Auf diese RFC-Dokumente können Sie direkt über das Web zugreifen, die URL lautet `http://www.ietf.org/`. In der Zwischenzeit sind einige Verfeinerungen am TCP/IP Protokoll vorgenommen worden, am grundlegenden Protokoll hat sich seit 1981 aber nichts geändert.

Hinweis

Die RFC-Dokumente beschreiben den Aufbau der Internet Protokolle. Falls Sie Ihr Know-how über ein bestimmtes Protokoll vertiefen wollen, ist das passende RFC-Dokument die richtige Anlaufstelle: `http://www.ietf.org/rfc.html`

Hinweis

Die in Tabelle 21.1 genannten Dienste stehen zur Verfügung, um Daten zwischen zwei Linuxrechnern über TCP/IP auszutauschen:

Tabelle 21.1: *Verschiedene Protokolle der TCP/IP Protokollfamilie*

Protokoll	Beschreibung
TCP	(engl. *Transmission control protocol*) Ein verbindungsorientiertes, gesichertes Protokoll. Die zu übertragenden Daten werden aus der Sicht der Applikation als Datenstrom verschickt und vom Betriebssystem selbst in das passende Übertragungsformat gebracht. Die Daten kommen bei der Zielapplikation auf dem Zielrechner als exakt der Datenstrom an, als der sie abgeschickt wurden. TCP stellt sicher, dass unterwegs keine Daten verloren gehen und nichts durcheinander kommt. TCP wird dort verwendet, wo die Reihenfolge der Daten wichtig ist und der Begriff Verbindung Sinn macht.

UDP	(engl. *User Datagram protocol*) Ein verbindungsloses, ungesichertes Protokoll. Die zu übertragenden Daten werden paketorientiert verschickt, die Datenpakete werden dabei schon von der Applikation erzeugt. Die Reihenfolge der Daten beim Empfänger ist nicht garantiert, ebenso kann es passieren, dass einzelne Datenpakete verloren gehen. UDP eignet sich für datensatzorientierte Applikationen und bietet kleinere Latenzzeiten als TCP.
ICMP	(engl. *Internet Control Message Protocol*) Im Wesentlichen ist das kein für den Benutzer verwendbares Protokoll, sondern ein spezielles Steuerprotokoll, das Fehlerzustände übermittelt und das Verhalten der an der TCP/IP-Datenübertragung beteiligten Rechner steuern kann. Zusätzlich wird durch ICMP noch ein spezieller Echo-Modus bereitgestellt, den man mit dem Programm ping prüfen kann.
IGMP	(engl. *Internet group management protocol*) Dieses Protokoll steuert das Verhalten von Rechnern bei der Verwendung von IP-Multicast. Leider kann IP-Multicasting in diesem Rahmen nicht vorgestellt werden.

Fast alle Hardwareprotokolle arbeiten paketorientiert. Die zu übertragenden Daten müssen in kleine „Päckchen“ gepackt werden und können nicht „in einem Rutsch“ verschickt werden. Deshalb arbeitet auch TCP/IP mit kleinen Datenpaketen. Die Maximalgröße eines TCP/IP Paketes ist knapp 64 Kilobyte. In der Praxis sind die Pakete normalerweise viel kleiner, da die Netzwerkhardware der limitierende Faktor ist. So ist die zulässige Maximalgröße eines Datenpaketes auf dem Ethernet ca. 1500 Byte. Dementsprechend wird die Paketgröße des TCP/IP Pakets begrenzt, wenn die Daten über ein Ethernet geschickt werden. Will man mehr Daten übertragen, müssen vom Betriebssystem entsprechend mehr Datenpakete verschickt werden.

21.1.1 Schichtenmodell

Über IP (engl. *Internet protocol*) findet eine ungesicherte Datenübertragung statt. TCP (engl. *Transmission control protocol*) ist gewissermaßen nur ein Aufsatz auf das darunter liegende IP, um eine gesicherte Übertragung der Daten zu garantieren. IP selbst ist wiederum ein Aufsatz auf das

darunter liegende, hardwareabhängige Protokoll, zum Beispiel Ethernet. Kenner sprechen hier vom „Schichtenmodell“. Vergleichen Sie hierzu die Abbildung 21.1.

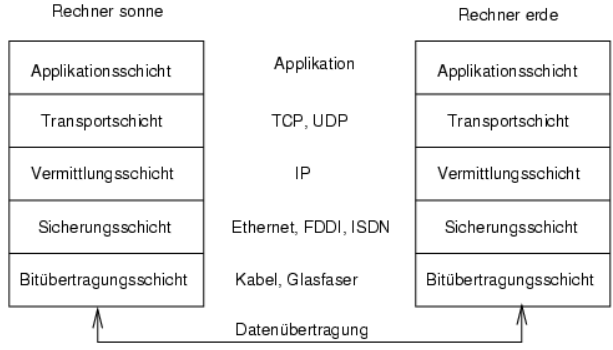

Abbildung 21.1: *Vereinfachtes Schichtenmodell für TCP/IP*

In der Abbildung sind jeweils ein oder zwei Beispiele für die jeweilige Schicht erwähnt. Wie Sie sehen, sind die Schichten nach „Abstraktionsebenen“ geordnet, die unterste Schicht ist sehr nah an der Hardware. Die oberste Schicht hingegen abstrahiert die darunter liegende Hardware nahezu vollständig. Jede der Schichten hat eine ganz spezielle Funktion, die zum Großteil schon aus der Bezeichnung hervorgeht. So wird das verwendete Netzwerk (zum Beispiel Ethernet) durch die Bitübertragungsschicht und die Sicherungsschicht verkörpert.

- Während sich Schicht 1 mit solchen Dingen wie Kabeltypen, Signalformen, Signalkodierung und ähnlichem beschäftigt ist Schicht 2 für das Zugriffsverfahren (Welcher Rechner darf wann Daten schicken?) und eine Fehlerkorrektur (Datensicherung - deshalb *Sicherungsschicht*) zuständig. Die Schicht 1 nennt man die *Bitübertragungsschicht*.
- Schicht 3 wiederum, die *Vermittlungsschicht* ist für die Datenübertragung über weite Strecken verantwortlich. Die Vermittlungsschicht stellt sicher, dass die Daten auch über weite Strecken beim richtigen Empfänger ankommen und zugestellt werden können.
- Schicht 4, die *Transportschicht*, ist für die Daten der Applikation verantwortlich und stellt sicher, dass die Daten in der richtigen Reihenfolge ankommen und nicht verloren gehen. Die Sicherungsschicht ist

nur dafür verantwortlich, dass die ankommenden Daten korrekt sind. Gegen das „Verlieren“ von Daten schützt die *Transportschicht*.

- Schicht 5 schließlich ist die Datenverarbeitung durch die Applikation selbst.

Damit jede der Schichten die ihr zugeteilte Aufgabe erfüllen kann, müssen zusätzliche Informationen der jeweiligen Schicht im Datenpaket im *Header*, dem Kopf des Datenpakets, gespeichert werden. Jede der Schichten fügt einen kleinen Datenblock, den sog. „Protokollkopf“ (engl. *Protocol header*), an das im Entstehen begriffene Paket vorne dran. Schauen wir uns also einmal ein beliebiges TCP/IP-Datenpaket an, das auf einem Ethernetkabel unterwegs ist, so setzt sich dieses wie in Bild 21.2 abgebildet zusammen.

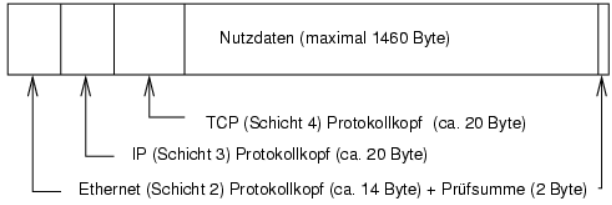

Abbildung 21.2: *TCP/IP Paket im Ethernet*

Wie Sie sehen, ist die Welt nicht perfekt und ohne Ausnahme. Die Prüfsumme der Sicherungsschicht befindet sich am Ende des Pakets und nicht am Anfang. Dies bringt aber für die Netzwerkhardware eine Vereinfachung. Die maximal mögliche Menge der Nutzdaten in einem Paket beträgt im Ethernet-Netzwerk 1460 Byte.

Möchte eine Applikation also Daten über das Netzwerk verschicken, durchlaufen die Daten die einzelnen Schichtebenen, die alle im Linuxkernel (Ausnahme Schicht 1: Netzwerkkarte) implementiert sind. Jede der Schichten ist dafür verantwortlich, die Daten so aufzubereiten, dass sie an die jeweils darunter liegende Schicht weitergereicht werden können. Die unterste Schicht ist schließlich für den eigentlichen Datenversand zuständig. Beim Empfang läuft das ganze nun umgekehrt ab. Wie bei den Schalen einer Zwiebel werden von jeder Schicht die Protokollköpfe von den Nutzdaten entfernt. Schicht 4 ist dann letztendlich dafür verantwortlich, die Daten für die Applikation auf dem Zielrechner bereitzustellen. Dabei kommuniziert eine Schicht immer nur mit der Schicht direkt über oder unter ihr. Für eine Applikation ist es also irrelevant, ob die Daten über ein

100-MBit/s-FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Umgekehrt ist es für die Datenübertragungsleitung egal, welche Daten eigentlich verschickt werden, solange sie richtig verpackt sind.

21.1.2 IP-Adressen und Routing

Hinweis

Die folgenden Abschnitte beschreiben IPv4-Netzwerke. Informationen zu seinem Nachfolgeprotokoll IPv6 bekommen Sie Abschnitt 21.2 auf Seite 463.

Hinweis

IP-Adressen

Jeder Computer im Internet hat eine eindeutige 32-Bit-Adresse. Diese 32 Bit bzw. 4 Byte werden normalerweise wie in Beispiel 21.1 in der zweiten Zeile abgebildet geschrieben.

Beispiel 21.1: *Schreibweise einer IP-Adresse*

```
IP-Adresse (binär):   11000000 10101000 00000000 00010100
IP-Adresse (dezimal):      192.     168.       0.      20
```

Die vier Bytes werden also im dezimalen Zahlensystem durch einen Punkt getrennt nebeneinander geschrieben. Die IP-Adresse ist einem Rechner bzw. einer Netzwerkschnittstelle zugeordnet, sie kann also nicht woanders auf der Welt nochmals verwendet werden. Ausnahmen von diesen Regeln gibt es zwar, spielen aber bei der folgenden Betrachtung erst einmal keine Rolle.

Auch die Ethernetkarte besitzt selbst eine eindeutige Adresse, die so genannte *MAC* (engl. *Media access control*) Adresse. Diese ist 48 Bit lang, weltweit eindeutig und wird vom Hersteller der Netzwerkkarte fest in der Hardware gespeichert. Durch die Vergabe der Adresse vom Hersteller ergibt sich aber ein fataler Nachteil: Die *MAC*-Adressen bilden kein hierarchisches System, sondern sind mehr oder weniger zufällig verteilt. Sie können daher nicht zur Adressierung eines weit entfernten Rechners verwendet

werden. Die *MAC*-Adresse spielt aber bei der Kommunikation von Rechnern in einem lokalen Netz eine entscheidende Rolle (und ist der Hauptbestandteil des Protokollkopfes von Schicht 2).

Zurück zu den IP-Adressen: Die Punkte deuten schon an, dass die IP-Adressen ein hierarchisches System bilden. Bis Mitte der 90er Jahre waren die IP-Adressen fest in Klassen eingeteilt. Dieses System erwies sich aber als zu unflexibel und daher wurde diese Aufteilung aufgegeben. Man verwendet nun „klassenloses Routing“ (CIDR (engl. *classless inter domain routing*)).

Netzmasken und Routing

Da der Rechner mit der IP-Adresse 192.168.0.0 erst einmal nicht wissen kann, wo sich der Rechner mit der IP-Adresse 192.168.0.20 befindet, wurden die Netzmasken erdacht.

Vereinfacht gesagt definiert die (Sub-)Netzmaske auf einem Rechner mit IP-Adresse, was „drinnen“ und was „draußen“ ist. Rechner, die sich „drinnen“ (Profis sagen: „im gleichen Subnetz“) befinden, können direkt angesprochen werden. Rechner, die sich „draußen“ („nicht im gleichen Subnetz“) befinden, müssen über ein so genanntes Gateway oder Router angesprochen werden. Da jedes Netzwerkinterface eine eigene IP-Adresse bekommen kann, ahnen Sie schon, dass es schnell beliebig kompliziert wird.

Bevor ein Netzwerkpaket auf die Reise geschickt wird, läuft folgendes im Rechner ab: Die Zieladresse wird mit der Netzmaske bitweise UND verknüpft. Daraufhin wird auch die Absendeadresse bitweise mit der Netzmaske UND verknüpft (siehe Tabelle 21.2). Stehen mehrere Netzwerkinterfaces zur Verfügung, werden in der Regel alle möglichen Absendeadressen überprüft.

Die Ergebnisse der UND-Verknüpfungen werden verglichen. Ergibt sich zwischen den Ergebnissen eine exakte Übereinstimmung, so befindet sich der Zielrechner im gleichen Subnetz. Ansonsten muss er über ein Gateway angesprochen werden. Das heißt, je mehr „1“ Bits sich in der Netzmaske befinden, desto weniger Rechner können direkt, sondern nur über ein Gateway angesprochen werden. Zur Veranschaulichung sind in Beispiel 21.2 mehrere Beispiele aufgeführt.

Beispiel 21.2: *Verknüpfungen der IP-Adressen mit der Netzmaske*

```
IP-Adresse (192.168.0.20):  11000000 10101000 00000000 00010100
Netzmaske (255.255.255.0):  11111111 11111111 11111111 00000000
_____________________________________________________________
```

```
Ergebnis (binär):           11000000 10101000 00000000 00000000
Ergebnis (dezimal):              192.     168.       0.       0

IP-Adresse (213.95.15.200): 11010101 10111111 00001111 11001000
Netzmaske  (255.255.255.0): 11111111 11111111 11111111 00000000
-----------------------------------------------------------------
Ergebnis (binär):           11010101 10111111 00001111 00000000
Ergebnis (dezimal):              213.      95.      15.       0
```

Die Netzmaske wird wieder – wie schon die IP-Adresse – in Form von durch Punkte getrennten Dezimalzahlen geschrieben. Da die Netzmaske auch ein 32-Bit-Wert ist, werden vier Zahlenwerte nebeneinander geschrieben. Welche Rechner Gateway sind oder welche Adressbereiche über welche Netzwerkschnittstelle erreichbar sind, muss vom Benutzer konfiguriert werden.

Um wieder ein Beispiel zu geben: Alle Rechner, die am gleichen Ethernetkabel angeschlossen sind, befinden sich in der Regel *im gleichen Subnetz* und sind direkt erreichbar. Auch wenn das Ethernet über Switches oder Bridges unterteilt ist, sind diese Rechner immer noch direkt erreichbar.

Wollen Sie eine längere Strecke überbrücken, ist das preiswerte Ethernet dafür nicht mehr geeignet. Sie müssen dann die IP-Pakete auf andere Hardware (zum Beispiel FDDI oder ISDN) weiterleiten. Solche Geräte heißen Router bzw. Gateway. Ein Linuxrechner kann diese Aufgabe selbstverständlich auch erledigen, die entsprechende Option wird mit `ip_forwarding` bezeichnet.

Ist ein Gateway konfiguriert, wird das IP-Paket an das passende Gateway geschickt. Dieses versucht, das Paket dann wiederum nach dem gleichen Schema weiterzuleiten. Das wiederholt sich auf jedem weiteren Rechner sooft, bis das Paket entweder den Zielrechner erreicht hat oder die „Lebenszeit“ TTL (engl. *time to live*) des Paketes verbraucht ist.

Tabelle 21.2: *Spezielle Adressen*

Adressart	**Beschreibung**
Netzwerkbasisadresse	Das ist die Netzmaske UND eine beliebige Adresse aus dem Netz, also das was in Beispiel 21.2 auf der vorherigen Seite unter `Ergebnis` abgebildet ist. Diese Adresse kann keinem Rechner zugewiesen werden.

Broadcastadresse	Sie heißt soviel wie: „Sprich alle Rechner in diesem Subnetz an“. Um sie zu erzeugen wird die Netzmaske binär invertiert und mit der Netzwerkbasisadresse ODER verknüpft. Obiges Beispiel ergibt also 192.168.0.255. Natürlich kann auch diese Adresse keinem Rechner zugewiesen werden.
Localhost	Die Adresse `127.0.0.1` ist auf jedem Rechner fest dem so genannten „Loopbackdevice“ zugewiesen. Über diese Adresse kann man eine Verbindung auf den eigenen Rechner aufbauen.

Da die IP-Adressen aber weltweit eindeutig sein müssen, können Sie natürlich nicht beliebige Adressen erfinden. Damit Sie aber trotzdem ein auf IP basierendes Netzwerk aufbauen können gibt es drei Adressbereiche, die Sie ohne weiteres verwenden können. Mit diesen können Sie allerdings nicht so ohne weiteres Verbindungen in das Internet aufbauen, da diese Adressen im Internet nicht weitergeleitet werden.

Dabei handelt es sich um diese Adressbereiche die in RFC 1597 definiert sind:

Tabelle 21.3: *Private IP-Adressbereiche*

Netzwerk/Netzmaske	Bereich
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x - 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

21.1.3 Domain Name System – DNS

DNS sorgt dafür, dass Sie sich nicht zwingend irgendwelche IP-Adressen merken müssen: Mit Hilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch eine Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise von einer speziellen Software namens bind. Der Rechner, der diese Umwandlung dann erledigt, nennt sich *Nameserver*. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandtei-

le durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Schauen wir uns einmal einen vollständigen Namen an, zum Beispiel `laurent.suse.de` geschrieben im Format `Rechnername.Domain`. Ein vollständiger Name – Experten sagen „fully qualified domain name“ oder kurz *FQDN* dazu – besteht aus einem Rechnernamen und einem Domainteil. Dabei wird der Domainteil aus einem frei wählbaren Anteil – im obigen Beispiel `suse` – und der so genannten *Top level domain*, *TLD* gebildet.

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen; seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (zum Beispiel `.info`, `.name`, `.museum` usw.).

In der Frühzeit des Internets (vor 1990) gab es hierzu eine Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge von am Internet angeschlossener Rechner als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Rechnernamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Nameserver, hält also nicht die Daten aller Rechner im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Nameserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die „Root-Nameserver“, die die Top level domains verwalten. Die Root-Nameserver werden vom Network Information Center (*NIC*) verwaltet. Der Root-Nameserver kennt die jeweils für eine Top level domain zuständigen Nameserver. Im Falle der deutschen Top level domain `de` ist das DE-NIC für die Domains zuständig, die mit der TLD `de` aufhören. Mehr Informationen zum DE-NIC erhalten Sie auf der Website `http://www.denic.de`, mehr Informationen zum Top level domain NIC erfahren Sie unter `http://www.internic.net`.

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Nameserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Nameservers erledigen Sie komfortabel mit Hilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass das zur Einwahl verwendete Protokoll die Adresse des Nameservers während der Einwahl mitliefert.

Aber nicht nur Rechnernamen können über DNS aufgelöst werden, DNS kann noch mehr. Zum Beispiel „weiß“ der Nameserver auch, welcher Rechner für eine ganze Domain E-Mails annimmt, der so genannte *Mail exchanger (MX)*.

Die Konfiguration des Nameserverzugriffs unter SUSE LINUX ist im Abschnitt 21.7 auf Seite 502 beschrieben.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm whois können Sie schnell herauskriegen, wer für eine bestimmte Domain verantwortlich ist.

21.2 IPv6 – Internet der nächsten Generation

Hinweis

S/390, zSeries: IPv6-Unterstützung

IPv6 wird von den CTC- und IUCV-Netzwerkverbindungen der IBM S/390 und zSeries Hardware nicht unterstützt.

Hinweis

Bedingt durch die Erfindung des WWW (engl. *World Wide Web*) ist das Internet und damit die Anzahl der Rechner, die TCP/IP „sprechen“, in den letzten zehn Jahren explosionsartig gewachsen. Seit der Erfindung des WWW durch Tim Berners-Lee 1990 am CERN (`http://public.web.cern.ch/`) ist die Zahl der Internet-Hosts von wenigen tausend auf mittlerweile ca. 100 Millionen angewachsen.

Wie Sie wissen, besteht eine IP-Adresse „nur“ aus 32 Bit. Viele IP-Adressen können durch organisatorische Bedingtheiten gar nicht verwendet werden, sie gehen verloren. Zur Erinnerung: Das Internet wird in Subnetze, also Teilnetze unterteilt. Diese bestehen immer aus einer Zweierpotenz minus zwei nutzbaren IP-Adressen. Ein Subnetz besteht also beispielsweise aus 2, 6, 14, 30 usw. IP-Adressen. Möchten Sie beispielsweise 128 Rechner an das Internet anbinden, so benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 nutzbar sind. Wie Sie oben gesehen haben, entfallen zwei der IP-Adressen aus einem Subnetz, nämlich die Broadcastadresse und die Netzwerkbasisadresse.

Um die absehbare Adressknappheit zu entschärfen, verwendet man unter dem momentan eingesetzten IPv4 Mechanismen wie DHCP oder NAT (engl. *Network Address Translation*). Beide Verfahren mildern zusammen mit der Konvention von öffentlichen und privaten Netzwerkadressbereichen die Adressnot im Internet. Nachteil dieser Methoden ist die teilweise sehr umständliche und wartungsintensive Konfiguration. Sie benötigen

zum korrekten Aufsetzen eines Rechners im IPv4-Netzwerk zahlreiche Informationen wie die eigene IP-Adresse, Subnetzmaske, Gatewayadresse und unter Umständen einen Nameserver. Alle diese Angaben müssen Sie „wissen“ und können Sie nirgendwoher ableiten.

Mit IPv6 gehören Adressknappheit und komplizierte Konfigurationen der Vergangenheit an. In den folgenden Abschnitten erfahren Sie mehr zu den Neuerungen und Vorteilen von IPv6 und über den Übergang von altem zum neuen Protokoll.

21.2.1 Vorteile von IPv6

Der wichtigste und augenfälligste Vorteil des neuen Protokolls ist die enorme Vergrößerung des verfügbaren Adressraums. Eine IPv6-Adresse enthält 128 Bit anstelle der traditionellen 32 Bit. Somit stehen viele Billiarden (!) IP-Adressen zur Verfügung.

IPv6-Adressen unterscheiden sich von ihren Vorgängern nicht nur in der Länge, auch ihre innere Struktur ist anders und erlaubt es, speziellere Informationen über das zugehörige System und sein Netzwerk zu kodieren. Mehr dazu unter Abschnitt 21.2.2 auf der nächsten Seite.

Weitere wichtige Vorteile des neuen Protokolls in Kurzform:

Autokonfiguration IPv6 setzt das „Plug and Play“-Prinzip im Netzwerk um. Ein frisch installiertes System integriert sich ohne weiteren Konfigurationsaufwand ins (lokale) Netz. Der Autokonfigurationsmechanismus des Terminals leitet die eigene Adresse aus den Informationen ab, die ihm über das „Neighbor Discovery Protocol“ (ND) von den benachbarten Routern zugespielt werden. Dieses Verfahren erfordert keinerlei Eingriff von Seiten des Administrators und hat gegenüber dem unter IPv4 genutzten Adressverteiler DHCP den weiteren Vorteil, dass die Wartung eines zentralen Servers mit den verfügbaren Adressen entfällt.

Mobilität IPv6 erlaubt es, dass einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zugeordnet werden. Somit haben Sie als Benutzer eines Systems einfach und ohne Zusatzaufwand Zugang zu mehreren verschiedenen Netzen. Sie können dies mit dem „Roaming“ in Mobilfunknetzen vergleichen: Befinden Sie sich mitsamt Ihrem Mobiltelefon im Ausland, bucht sich das Handy automatisch in das fremde Netz ein. Egal, wo Sie sind, Ihre Erreichbarkeit unter Ihrer normalen Telefonnummer ist gewährleistet und Sie telefonieren im fremden Netz, als wäre es Ihr Heimatnetz.

Sichere Kommunikation Während sichere Kommunikation unter IPv4 nur als Zusatzfunktion zu realisieren war, ist IPSec und damit die sichere Kommunikation zwischen zwei Systemen über einen Tunnel durch das unsichere Internet in IPv6 bereits enthalten.

Kompatibilität zum Vorgänger Ein schneller Umstieg des gesamten Internets von IPv4 auf IPv6 ist nicht realistisch. Deshalb ist es wichtig, dass beide Versionen im Internet und sogar auf einem System koexistieren können. Die Koexistenz beider im Internet ist durch die Verwendung kompatibler Adressen (IPv4-Adressen lassen sich einfach in IPv6-Adressen umsetzen) und die Verwendung verschiedener „Tunnel" gesichert (siehe Abschnitt 21.2.3 auf Seite 470). Über „Dual-Stack-IP" ist die Unterstützung beider Protokolle auf dem einzelnen System möglich. Jedes der beiden Protokolle verwendet einen eigenen Netzwerkstack, so dass sich die beiden Protokollversionen nicht gegenseitig in die Quere kommen.

Multicasting – maßgeschneidertes Dienstangebot Während unter IPv4 einige Dienste (zum Beispiel SMB) ihre Pakete per Broadcast an alle Teilnehmer des lokalen Netzes senden mussten, ist unter IPv6 ein viel differenzierteres Vorgehen möglich. Mit Hilfe von Multicast kann eine Gruppe von Rechnern auf einmal angesprochen werden, also nicht alle auf einmal („broadcast"), oder nur einer („unicast"), sondern eben ein paar. Welche das sind, hängt von der Anwendung ab. Es gibt aber auch ein paar wohldefinierte Multicastgruppen, beispielsweise „alle Nameserver" (engl. *all nameservers multicast group*), oder „alle Router" (engl. *all routers multicast group*).

21.2.2 Das Adresssystem von IPv6

Wie bereits erwähnt, hat das bisher verwendete IP-Protokoll zwei schwerwiegende Nachteile. Zum einen gehen die verfügbaren IP-Adressen langsam aus und zum anderen ist die Netzwerkkonfiguration und das Verwalten von Routingtabellen immer komplizierter und wartungsintensiver. Dem ersten Problem begegnet IPv6 mit der Erweiterung des Adressraums auf 128 Bit. Die Lösung für das zweite Problem liegt der hierarchischen Adressstruktur, ausgeklügelten Mechanismen zur Adresszuweisung im Netz und der Möglichkeit des „Multi-Homings" (mehrere Adressen pro Schnittstelle mit Zugang zu verschiedenen Netzwerken).

In Zusammenhang mit IPv6 sollten Sie folgende drei Adresstypen unterscheiden können:

unicast Adressen dieses Typs gehören zu genau einer Netzwerkschnittstelle. Pakete mit einer Adresse dieses Typs werden an genau einen Empfänger ausgeliefert. Unicast-Adressen werden verwendet, um einzelne Rechner im lokalen Netz oder Internet anzusprechen.

multicast Adressen dieses Typs weisen auf eine Gruppe von Schnittstellen. Pakete mit einer Adresse dieses Typs werden an alle Empfänger zugestellt, die zu dieser Gruppe gehören. Multicast-Adressen werden vorwiegend von bestimmten Netzwerkdiensten benutzt, um gezielt bestimmte Gruppen von Rechnern zu adressieren.

anycast Adressen dieses Typs weisen auf eine Gruppe von Schnittstellen. Pakete mit einer Adresse dieses Typs werden an den Ängehörigen der Gruppe ausgeliefert, der nach den Begriffen des verwendeten Routingprotokolls dem Absender am nächsten ist. Anycast-Adressen werden verwendet, um Terminal das Auffinden eines Servers mit einem bestimmten Dienstangebot in ihrem Netzbereich zu finden. Alle Server eines Typs erhalten die gleiche Anycast-Adresse. Fordert der Terminal einen Dienst an, antwortet derjenige Server, der nach Einschätzung des Routingprotokolls dem Host am nächsten liegt. Sollte dieser Server ausfallen, wird automatisch der zweitnächste verwendet ....

Aufbau einer IPv6-Adresse

Eine IPv6-Adresse setzt sich aus acht Blöcken zu je 16 Bit zusammen, die durch `:` (Doppelpunkt) getrennt werden und in Hexadezimalschreibweise dargestellt werden. Führende Null-Bytes in einer Gruppe dürfen weggelassen werden, nicht aber inmitten oder am Ende einer Gruppe. Mehr als vier Null-Bytes direkt hintereinander kann man durch das Auslassungszeichen `::` überspringen. Allerdings ist nur ein Auslassungszeichen in einer Adresse erlaubt. Dieser Vorgang des Auslassens wird in Englisch mit „collapsing“ bezeichnet. In Ausgabe 21.3 ist dieser Vorgang anhand dreier äquivalenter Schreibweisen ein und derselben Adresse dargestellt.

Beispiel 21.3: *Beispiel einer IPv6-Adresse*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

Jeder Teil einer IPv6-Adresse hat eine definierte Bedeutung. Die ersten Bytes bilden einen Präfix und geben den Typ der Adresse an. Der Mittelteil adressiert ein Netzwerk oder ist bedeutungslos und den Schluss der

Adresse bildet der Hostteil. Netzmasken definieren sich unter IPv6 über die Länge des Präfix, die per / am Ende der Adresse mit angegeben wird. Eine Adressdarstellung wie in Ausgabe 21.4 besagt, dass die letzten 64 Bit den Hostteil und die vorderen 64 Bit den Netzwerkteil der Adresse bilden. Anders gesagt bedeutet die `64`, dass von links her die Netzmaske mit 1 Bits aufgefüllt wird. Es gibt in der Netzmaske also 64 1 Bits. Wie bei IPv4 wird durch eine UND-Verknüpfung der Netzmaske mit der IP-Adresse bestimmt, ob sich ein Rechner im gleichen oder in einem anderen Subnetz befindet.

Beispiel 21.4: *IPv6-Adresse mit Präfixangabe*

```
fe80::10:1000:1a4/64
```

IPv6 kennt verschiedene Präfixe mit definierter Bedeutung (siehe Tabelle 21.4).

Tabelle 21.4: *verschiedene IPv6-Präfixe*

Präfix (hexadez.)	Verwendung
`00`	IPv4 Adressen und IPv4 über IPv6-Kompatibilitätsadressen. Es handelt sich um eine zu IPv4 kompatible Adresse. Ein geeigneter Router muss das IPv6-Paket noch in IPv4 verwandeln. Weitere Spezialadressen (zum Beispiel Loopback Device) sind ebenfalls mit diesem Präfix ausgestattet.
erste Ziffer `2` oder `3`	(engl. *Aggregatable Global Unicast Address*). Wie bisher auch können Sie bei IPv6 Teilnetze zugewiesen bekommen. Aktuell gibt es folgende Adressräume: `2001::/16` (*production quality address space*) und `2002::/16` (*6to4 address space*).
`fe80::/10`	(engl. *link-local*) Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
`fec0::/10`	(engl. *site-local*) Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb einer Organisation. Damit entsprechen diese Adressen den bisherigen „privaten“ Netzen (beispielsweise `10.x.x.x`).
`ff`	(engl. *multicast*) IPv6-Adressen, die mit `ff` anfangen, sind Multicastadressen.

Unicastadressen folgen einem dreigeteilten Aufbauprinzip:

Public Topology Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixes enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site Topology Der zweite Teil enthält Routinginformationen über das Subnetz, in dem das Paket zugestellt werden soll.

Interface ID Der dritte Teil identifiziert eindeutig die Schnittstelle, an die das Paket gerichtet ist. Dies erlaubt, die MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration der Rechner sehr. In Wirklichkeit werden sogar die ersten 64 Bit zu einem so genannten `EUI-64`-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen, die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (PPP- und ISDN-Verbindungen!) ein `EUI-64`-Token zuzuweisen.

► **S/390, zSeries**
Geräte ohne MAC-Adresse sind auf IBM S/390 und zSeries IUCV und CTC (Point-to-Point). ◄

Abgeleitet aus diesem Grundaufbau werden fünf verschiedene Typen von Unicastadressen unterschieden:

`::` (unspecified) diese Adresse verwendet ein Rechner als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und noch keine Informationen über die eigene Adresse hat.

`::1` (loopback) Adresse des Loopback-Devices.

IPv4 kompatible Adresse Die IPv6-Adresse wird aus der IPv4-Adresse und einem Präfix von 96 0-Bits am Beginn der Adresse zusammengestellt. Dieser Typ der Kompatibilitätsadressen wird beim Tunneling verwendet (siehe Abschnitt 21.2.3 auf Seite 470). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich im reinen IPv4-Netz befinden.

IPv6 gemappte IPv4-Adresse Dieser Adresstyp gibt die IPv6-Adresse eines reinen IPv4-Rechners an.

Lokale Adressen Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

link-local Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch einen speziellen Präfix (`fe80::/10`) und die Interface-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus aussagefreien Nullbytes. Diese Art von Adresse wird von den Autokonfigurationsmethoden verwendet, um Rechner im gleichen Subnetz anzusprechen.

site-local Dieser Adresstyp darf zwischen einzelnen Subnetzen geroutet werden, aber nicht außerhalb einer Organisation (engl. *site*) ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten Adressen des IPv4. Neben einem definierten Präfix (`fec0::/10`) und der Interface-ID enthalten diese Adressen ein 16 Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Bytes aufgefüllt.

Zusätzlich gibt es in IPv6 eine neue Erfindung: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines davon kann mit Hilfe der MAC-Adresse und einem bekannten Präfix zu einem vollautomatisch konfigurierten Netz zusammengestellt werden, und ohne weitere Konfigurationsarbeiten sind damit direkt nach dem Starten von IPv6 alle Rechner im lokalen Netz erreichbar (sog. „Link-local-Adresse“). Die MAC-Adresse als Bestandteil der IP-Adresse macht jede dieser Adressen global unterscheidbar. Einzig die Teile der „Site Topology“ oder „Public Topology“ können variieren, je nachdem in welchem Netz dieser Rechner aktuell zu erreichen ist.

„Bewegt“ sich ein Rechner zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine „Home Address“ beinhaltet neben seiner Interface-ID die Informationen zu seinem Heimatnetz, in dem er normalerweise betrieben wird und das entsprechende Präfix. Die „Home Address“ ist statisch und wird nicht verändert. Alle Pakete, die für diesen Rechner bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, über *Stateless Autoconfiguration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner „Home

Address“ eine oder mehrere weitere Adressen, die in die fremden Netze gehören, in denen er sich bewegt. Diese Addressen heißen „Care-of Address“. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine „Home Address“ gerichtete „nachsendet“, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einem IPv6-Szenario vom „Home Agent“ übernommen. Er stellt alle Pakete, die an die Heimatadresse des mobilen Rechners gerichtet sind, über einen Tunnel zu. Pakete, die als Zieladresse die „Care-of Address“ tragen, können ohne Umweg über den Home Agent zugestellt werden.

21.2.3 IPv4 versus IPv6 – Wandern zwischen den Welten

Der Umstieg aller Rechner im Internet von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden altes und neues Protokoll noch eine ganze Weile nebeneinanderher existieren. Die Koexistenz auf einem Rechner ist per „Dual Stack“ gelöst, es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6 über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Verwendung von Kompatibilitätsadressen (siehe Abschnitt 21.2.2 auf Seite 466) sind hier die Methoden der Wahl.

Einzelne IPv6-Inseln im (weltweiten) IPv4-Netz tauschen ihre Daten über Tunnel aus. Beim Tunneling werden IPv6-Pakete in IPv4-Pakete verpackt, um sie über ein reines IPv4-Netzwerk transportieren zu können. Ein Tunnel ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei muss die IPv6-Zieladresse (oder das entsprechende Präfix) angegeben werden, an die die verkappten IPv6-Pakete gerichtet sind und die entfernte IPv4-Adresse, an der die getunnelten Pakete in Empfang genommen werden sollen. Im einfachsten Fall konfigurieren Administratoren solche Tunnel zwischen ihren Netzwerken *manuell* und nach Absprache. Solches Tunneling wird *statisches* Tunneling genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden drei verschiedene Verfahren entwickelt, die *dynamisches* Tunneling erlauben:

6over4 IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (engl. *Local Area Network*). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteil dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese

Lösung eignet sich für kleinere Firmen- oder Institutsnetzwerke, die die Möglichkeit von IP-Multicasting bieten. Das zugrundeliegende RFC ist RFC2529.

6to4 Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können IPv6-Inseln über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es betreffend der Kommunikation zwischen IPv6-Inseln und dem Internet einige Probleme. Das zugrundeliegende RFC ist RFC3056.

IPv6 Tunnel Broker Dieser Ansatz sieht spezielle Server vor, die für den Benutzer automatisch Tunnel anlegen. Das zugrundeliegende RFC ist RFC3053.

Hinweis

Die 6Bone Initiative

Mitten im „altmodischen" Internet existiert mit *6Bone* (`www.6bone.net`) ein weltweit verteiltes Netzwerk von IPv6-Subnetzen, die über Tunnel miteinander verbunden sind. Innerhalb des 6Bone-Netzes wird IPv6 getestet. Softwareentwickler und Provider, die IPv6-Dienste entwickeln oder anbieten, können diese Testumgebung nutzen, um wichtige Erfahrungen mit dem neuen Protokoll zu bekommen. Weitere Informationen finden Sie auf den Projektseiten von 6Bone.

Hinweis

21.2.4 Weiterführende Literatur und Links zu IPv6

Natürlich kann und will der obige Überblick keine vollständige Einführung zum sehr umfangreichen Thema IPv6 sein. Zum tieferen Einstieg in IPv6 können Sie die folgende Onlineliteratur und Bücher zu Rate ziehen:

`http://www.ngnet.it/e/cosa-ipv6.php`
Artikelserie mit sehr guten Beschreibungen zu den Grundlagen von IPv6. Gut geeignet für einen Einstieg ins Thema.

`http://www.bieringer.de/linux/IPv6/`
Linux-IPv6-HOWTO und viele Links.

`http://www.6bone.de/` Anschluss an das IPv6 über einen Tunnel bekommen.

http://www.ipv6.org/ Alles rund um IPv6.

RFC 2640 Das einführende RFC zum Thema IPv6.

IPv6 Essentials Englischsprachiger Überblick zum Thema IPv6. Hagen, Silvia: *IPv6 Essentials*. O'Reilly & Associates, 2002. - (ISBN 0-596-00125-8).

21.3 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte stets die zweite Wahl sein. Wir empfehlen, YaST zu benutzen. Wesentlich ist, dass alle Netzwerk-Interfaces mit dem Skript `/sbin/ifup` aufgesetzt werden. Zum Anhalten oder Prüfen eines Interfaces gibt es `ifdown` und `ifstatus`.

Wenn Sie nur fest eingebaute Netzwerkkarten haben, genügt es die Interfaces über ihren Namen zu konfigurieren. Mit `ifup eth0`, `ifstatus eth0` und `ifdown eth0` starten, prüfen und stoppen Sie das Netzwerkinterface `eth0`. Die verwendeten Konfigurationsdaten liegen unter `/etc/sysconfig/network/ifcfg-eth0`. `eth0` ist hier sowohl der Interface-Name als auch der Name für die Netzwerkkonfiguration.

Die Netzwerkkonfiguration kann alternativ auch der Hardware-Adresse (MAC-Adresse) einer Netzwerkkarte zugeordnet werden. Dazu wird eine Konfigurationsdatei `ifcfg-<HardwareadresseohneDoppelpunkte>` verwendet. Die Buchstaben der Hardware-Adresse müssen hier klein geschrieben werden, so wie sie von `ip link` ausgegeben wird (`ifconfig` verwendet große Buchstaben). Wenn `ifup` eine Konfigurationsdatei passend zur Hardware-Adresse findet, wird ein möglicherweise auch vorhandenes `ifcfg-eth0` ignoriert. Gleiches gilt für hotplug Netzwerkkarten.

Mit hotplugfähigen Netzwerkkarten wird es ein wenig komplizierter. Wenn Sie keine solche Karte besitzen, können Sie beim Abschnitt 21.3.1 auf der nächsten Seite weiterlesen.

Da bei hotplugfähigen Netzwerkkarten die Zuordnung des Interface-Namen zur Karte eher zufällig ist, werden die Konfigurationen für eine solche Karte nicht unter dem Interface-Namen abgelegt, sondern unter einem Bezeichner, der die Art der verwendeten Hardware und den Anschlusspunkt beschreibt, im Folgenden Hardwarebeschreibung genannt. `ifup` muss in diesem Fall mit zwei Argumenten aufgerufen werden, der genauen Hardwarebeschreibung und dem gegenwärtigen Interface-Namen. Anschließend wird von `ifup` die Konfiguration ermittelt, die möglichst genau auf die Hardwarebeschreibung passt.

Hinweis

Hotplugfähige Netzwerkkarten auf IBM S/390 und zSeries

Grundsätzlich sind die Netzwerkkarten auf IBM S/390und zSeries hotplugfähig. Die automatische Konfiguration per DHCP wie bei PCMCIA-Karten von PCs ist auf diesen Plattformen nicht möglich. Die Karten werden erkannt, müssen aber anschließend manuell konfiguriert werden. Das folgende Beispiel bezieht sich ausschließlich auf Hardware mit PCMCIA-Unterstützung.

Hinweis

Als Beispiel dient ein Laptop mit zwei PCMCIA-Steckplätzen und einer PCMCIA Ethernet Netzwerkkarte. Zusätzlich gibt es in diesem Gerät noch eine festeingebaute Netzwerkkarte, die als Interfacenamen `eth0` erhält. Wenn die PCMCIA-Karte im Steckplatz `0` steckt, lautet ihre Hardwarebeschreibung `eth-pcmcia-0`. Der cardmgr oder das Hotplug-Netzwerkscript rufen nun `ifup eth-pcmcia-0 eth1` auf. Nun sucht `ifup`, ob es unter `/etc/sysconfig/network/` eine Datei `ifcfg-eth-pcmcia-0` gibt. Wenn nicht, wird weiter nach `ifcfg-eth-pcmcia`, `ifcfg-pcmcia-0`, `ifcfg-pcmcia`, `ifcfg-eth1` und `ifcfg-eth` gesucht. Die zuerst gefundene Datei wird zur Konfiguration verwendet. Wenn also eine Netzwerkkonfiguration angelegt werden soll, die für alle PCMCIA-Netzwerkkarten (in allen Steckplätzen) gelten soll, muss diese `ifcfg-pcmcia` heißen. Diese würde dann für `eth-pcmcia-0` genauso wie für eine Tokenringkarte in Steckplatz 1 `tr-pcmcia-1` verwendet.

YaST geht bei der Konfiguration von hotplugfähigen Karten einen Umweg. Dort werden Konfigurationen für solche Karten durchnummeriert. Deshalb schreibt YaST die Einstellungen für eine PCMCIA-Karte immer nach `ifcfg-eth-pcmcia-<laufendeNummer>`. Damit diese Konfiguration dann trotzdem für alle Steckplätze funktioniert, wird noch ein Link `ifcfg-eth-pcmcia` auf diese Datei angelegt. Dies sollten Sie beachten, wenn Sie teilweise mit und teilweise ohne YaST konfigurieren.

21.3.1 Konfigurationsdateien

Dieser Abschnitt gibt eine Übersicht über die Netzwerkkonfigurationsdateien und erklärt ihre Funktion sowie das verwendete Format.

/etc/syconfig/hardware/*

In diesem Verzeichnis findet sich pro Gerät (Netzwerkkarte) eine Datei, die die entsprechenden Konfigurationsparameter (Kernelmodul, Startmodus und Skriptzuordnungen etc.) enthält.

/etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die Daten, die spezifisch für ein Netzwerk-Interface sind. Sie können nach dem Interface-Namen benannt sein (`ifcfg-eth2`), nach der Hardware-Adresse einer Netzwerkkarte (`ifcfg-000086386be3`) oder nach einer Hardware-Beschreibung für eine Karte (`ifcfg-usb`). Sollen Netzwerkaliase verwendet werden, heißen die dazu nötigen Dateien einfach `ifcfg-eth2:1` oder `ifcfg-usb:1`. Das Skript `ifup` bekommt neben dem Interface-Namen bei Bedarf auch eine genaue Hardwarebeschreibung und sucht dann die am besten passende Datei zur Konfiguration aus.

► **S/390, zSeries**
IBM S/390 und zSeries unterstützen kein USB. Namensgebung der Interface-Dateinamen und Netzwerkaliase enthalten S/390-spezische Bezeichner wie `qeth` o.ä. . ◄

Die Dateien enthalten die IP-Adresse (`BOOTPROTO=static`, `IPADDR=10.10.11.214`) oder die Anweisung, DHCP zu verwenden (`BOOTPROTO=`"dhcp"). Die IP-Adresse sollte die Netzmaske bereits enthalten (`IPADDR=`"10.10.11.214/16"). Die vollständige Liste von Variablen enthält die Manpage zu `ifup`. Es können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden, wenn eine sonst allgemeine Einstellung nur für ein Interface verwendet werden soll.

/etc/sysconfig/network/config,dhcp,wireless

Die Datei `config` enthält allgemeine Einstellungen zum Verhalten von `ifup`, `ifdown` und `ifstatus`. Sie ist vollständig kommentiert. Ebenso gibt es Kommentare in `dhcp` und `wireless`, wo allgemeine Einstellungen zu DHCP und Funknetzwerkkarten Platz finden. Alle Variablen aus diesen Dateien können auch in `ifcfg-*` verwendet werden und haben dort natürlich Vorrang.

/etc/resolv.conf

Wie bereits die Datei `/etc/host.conf`, so spielt auch diese Datei in Bezug auf Auflösung von Rechnernamen durch die *resolver*–Bibliothek eine Rolle.

In dieser Datei wird angegeben, welcher Domain der Rechner angehört (Schlüsselwort `search`) und wie die Adresse des Nameservers ist (Schlüsselwort `nameserver`), der angesprochen werden soll. Es können mehrere

Domainnamen angegeben werden. Beim Auflösen eines nicht voll qualifizierten Namens wird versucht, durch Anhängen der einzelnen Einträge in `search` einen gültigen, voll qualifizierten Namen zu erzeugen. Mehrere Nameserver können durch mehrere Zeilen, die mit `nameserver` beginnen, bekannt gemacht werden. Kommentare werden wieder mit # eingeleitet.

Ein Beispiel für `/etc/resolv.conf` zeigt Datei 21.5.

Beispiel 21.5: `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use sonne (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

YaST trägt hier den angegebenen Nameserver ein!

Einige Dienste wie pppd (wvdial), ipppd (isdn), dhcp (dhcpcd und dhclient), pcmcia und hotplug modifizieren die Datei `/etc/resolv.conf` über das Skript `modify_resolvconf`.

Wenn die Datei `/etc/resolv.conf` durch dieses Skript vorübergehend modifiziert wurde, enthält sie einen definierten Kommentar, der Auskunft darüber gibt, welcher Dienst sie modifiziert hat, wo die ursprüngliche Datei gesichert ist und wie man die automatischen Modifikationen abstellen kann.

Wenn `/etc/resolv.conf` mehrmals modifiziert wird, wird diese Verschachtelung von Modifikationen auch dann wieder sauber abgebaut, wenn sie in einer anderen Reihenfolge zurückgenommen werden; dies kann bei isdn, pcmcia und hotplug durchaus vorkommen.

Wenn ein Dienst nicht sauber beendet wurde, kann mit Hilfe des Skripts `modify_resolvconf` der Ursprungszustand wiederhergestellt werden. Beim Booten wird geprüft, ob eine modifizierte `resolv.conf` stehen geblieben ist (z. B. wegen Systemabsturz). Dann wird die ursprüngliche (unmodifizierte) `resolv.conf` wiederhergestellt.

YaST findet mittels `modify_resolvconf check` heraus, ob `resolv.conf` modifiziert wurde, und dann den Benutzer warnen, dass seine Änderungen nach der Restauration wieder verloren sein werden. Ansonsten verwendet YaST `modify_resolvconf` nicht, das heißt eine Änderung der Datei resolv.conf mittels YaST und eine manuelle Änderung sind äquivalent. Beides entspricht einer gezielten und dauerhaften Änderung, während eine Änderung durch einen der genannten Dienste nur vorübergehend ist.

/etc/hosts

In dieser Datei (siehe Datei 21.6) werden Rechnernamen IP–Adressen zugeordnet. Wird kein Nameserver verwendet, müssen hier alle Rechner aufgeführt werden, zu denen eine IP–Verbindung aufgebaut werden soll. Je Rechner wird eine Zeile bestehend aus IP-Adresse, dem voll qualifizierten Hostnamen und dem Rechnernamen (zum Beispiel `erde`) in die Datei eingetragen. Die IP–Adresse muss am Anfang der Zeile stehen, die Einträge werden durch Leerzeichen bzw. Tabulatoren getrennt. Kommentare werden durch # eingeleitet.

Beispiel 21.6: `/etc/hosts`

```
127.0.0.1 localhost
192.168.0.20 sonne.example.com sonne
192.168.0.0 erde.example.com erde
```

/etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen (siehe Datei 21.7).

Beispiel 21.7: `/etc/networks`

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

Das Auflösen von Namen – das heisst das Übersetzen von Rechner- bzw. Netzwerknamen über die *resolver*-Bibliothek – wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die gegen die libc4 oder die libc5 gelinkt sind; für aktuelle glibc-Programme vgl. die Einstellungen in `/etc/nsswitch.conf`! Ein Parameter muss in einer eigenen Zeile stehen, Kommentare werden durch # eingeleitet. Die möglichen Parameter zeigt Tabelle 21.5 auf der nächsten Seite.

Tabelle 21.5: *Parameter für /etc/host.conf*

order *hosts*, *bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente sind (durch Leerzeichen oder Kommata voneinander getrennt): *hosts*: Durchsuchen der Datei `/etc/hosts` *bind*: Ansprechen eines Nameservers *nis*: Über NIS
multi *on*/*off*	Bestimmt, ob ein in `/etc/hosts` eingetragener Rechner mehrere IP-Adressen haben darf.
nospoof *on* spoofalert *on*/*off*	Diese Parameter beeinflussen das *spoofing* des Nameservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration.
trim `domainname`	Der angegebene Domainname wird vor dem Auflösen des Rechnernamens von diesem abgeschnitten (insofern der Rechnername diesen Domainnamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domain stehen, diese aber auch mit angehängtem Domainnamen erkannt werden sollen.

Ein Beispiel für `/etc/host.conf` zeigt Datei 21.8.

Beispiel 21.8: *`/etc/host.conf`*

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

Mit der GNU C Library 2.0 hat der Name Service Switch (NSS) Einzug gehalten (vgl. die Manpage von `man 5 nsswitch.conf`, sowie ausführli-

cher *The GNU C Library Reference Manual*, Kapitel „System Databases and Name Service Switch“ >).

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` zeigt Datei 21.9. Kommentare werden durch # eingeleitet. Dort bedeutet zum Beispiel der Eintrag bei der Datenbank `hosts`, dass nach `/etc/hosts` (`files`) eine Anfrage über DNS (vgl. Abschnitt 21.7 auf Seite 502) losgeschickt wird.

Beispiel 21.9: *`/etc/nsswitch.conf`*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Die über NSS verfügbaren Datenbanken sind in Tabelle 21.6 genannt. Zusätzlich sind in Zukunft `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten.

Tabelle 21.6: *Über /etc/nsswitch.conf verfügbare Datenbanken*

`aliases`	Mail-Aliase, von `sendmail` verwendet; vgl. die Manpage `man 5 aliases`.
`ethers`	Ethernet-Adressen.
`group`	Für Benutzergruppen, von `getgrent` verwendet; vgl. die Manpage `man 5 group`.
`hosts`	Für Hostnamen und IP-Adressen, von `gethostbyname` und ähnlichen Funktionen verwendet.
`netgroup`	Im Netzwerk gültige Liste von Hosts und Benutzern, um Zugriffsrechte zu steuern; vgl. die Manpage `man 5 netgroup`.

networks	Netzwerknamen und -adressen, von getnetent verwendet.
passwd	Benutzerpasswörter, von getpwent verwendet; vgl. die Manpage man 5 passwd.
protocols	Netzwerk-Protokolle, von getprotoent verwendet; vgl. die Manpage man 5 protocols.
rpc	Remote Procedure Call-Namen und -Adressen, von getrpcbyname und ähnlichen Funktionen verwendet.
services	Netzwerkdienste, von getservent verwendet.
shadow	Shadow-Passwörter der Benutzer, von getspnam verwendet; vgl. die Manpage man 5 shadow.

Die Konfigurationsmöglichkeiten der NSS-Datenbanken stehen in Tabelle 21.7.

Tabelle 21.7: *Konfigurationsmöglichkeiten der NSS-Datenbanken*

files	direkt auf Dateien zugreifen, zum Beispiel auf /etc/aliases.
db	über eine Datenbank zugreifen.
nis	NIS, vgl. Abschnitt 21.9 auf Seite 553.
nisplus	
dns	Nur bei hosts und networks als Erweiterung verwendbar.
compat	Nur bei passwd, shadow und group als Erweiterung verwendbar.

Zusätzlich ist es möglich, unterschiedliche Reaktionen bei bestimmten Lookup-Ergebnissen auszulösen; Details sind der Manpage man 5 nsswitch.conf zu entnehmen.

/etc/nscd.conf

Über diese Datei wird der nscd (engl. *Name Service Cache Daemon*) konfiguriert (vgl. man 8 nscd und die man 5 nscd.conf). Per default werden die Einträge von passwd und groups gecached. hosts wird nor-

malerweise nicht gecached, da sich der Rechner dann nicht mehr auf „forward/reverse lookups“ dieses Namensdienstes verlassen kann. Statt dem nscd diese Aufgabe zu übertragen, sollten sie einen „caching“ Nameserver einrichten.

Wenn beispielsweise das Caching für `passwd` aktiviert ist, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten des nscd mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

/etc/HOSTNAME

Hier steht der Name des Rechners, also nur der Hostname ohne den Domainnamen. Diese Datei wird von verschiedenen Skripten während des Starts des Rechners gelesen. Sie darf nur eine Zeile enthalten, in der der Rechnername steht!

21.3.2 Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die während des Hochfahrens des Rechners die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Multiuser-Runlevel* übergeht (vgl. Tabelle 21.8).

Tabelle 21.8: *Einige Startup-Skripten der Netzwerkprogramme*

`/etc/init.d/network`	Dieses Skript übernimmt die Konfiguration der Netzwerk Hard- und Software während der Startphase des Systems.
`/etc/init.d/xinetd`	Startet den xinetd. Der xinetd kann verwendet werden, um bei Bedarf Serverdienste auf dem System zur Verfügung zu stellen. Beispielsweise kann er den vsftpd starten, sobald eine FTP-Verbindung initiiert wird.
`/etc/init.d/portmap`	Startet den Portmapper, der benötigt wird, um RPC-Server verwenden zu können, wie zum Beispiel einen NFS-Server.
`/etc/init.d/nfsserver`	Startet den NFS-Server.
`/etc/init.d/postfix`	Kontrolliert den postfix-Prozess.

`/etc/init.d/ypserv`	Startet den NIS-Server.
`/etc/init.d/ypbind`	Startet den NIS-Client.

21.4 Die Einbindung ins Netzwerk

TCP/IP ist inzwischen das Standard-Netzwerkprotokoll, über das alle modernen Betriebssysteme mit TCP/IP kommunizieren können. Dennoch unterstützt Linux auch noch andere Netzwerkprotokolle, beispielsweise das (früher) von Novell Netware verwendete IPX oder das von Macintosh-Rechnern verwendete Appletalk. In diesem Rahmen besprechen wir nur die Integration eines Linux-Rechners in ein TCP/IP-Netzwerk. Wenn Sie exotische Arcnet, Token-Ring oder FDDI-Netzwerkkarten einbinden wollen, finden Sie weiterführende Hilfe hierzu in den Kernelquellen `/usr/src/linux/Documentation`, die Sie separat mit dem Paket `kernel-source` installieren.

21.4.1 Vorbereitungen

Der Rechner muss über eine unterstützte Netzwerkkarte verfügen. Üblicherweise wird die Netzwerkkarte schon bei der Installation erkannt und der passende Treiber eingebunden. Ob Ihre Karte korrekt eingebunden wurde, können Sie unter anderem daran sehen, dass die Ausgabe des Kommandos `ifstatus eth0` das Netzwerk-Device `eth0` anzeigt.

► **S/390, zSeries**
Auf IBM S/390 und zSeries können neben `eth0` noch `hsi0`, `ctc0` und `iuvc0` verwendet werden. ◄

Wenn der Kernel-Support für die Netzwerkkarte als Modul realisiert wird – so wie es beim SUSE-Kernel standardmäßig der Fall ist –, dann muss der Name des Moduls als Alias in der `/etc/modprobe.conf` eingetragen werden. Dies geschieht automatisch, wenn im linuxrc während der Erstinstallation der Treiber-Support für die Netzwerkkarte geladen wird. Nachträglich lässt sich diese Aufgabe von YaST aus erledigen.

Bei hotplugfähigen Netzwerkkarten (zum Beispiel PCMCIA oder USB) werden die Treiber beim Einstecken automatisch ermittelt; es muss dazu nichts konfiguriert werden.

Hinweis

S/390, zSeries: Hotplugfähige Netzwerkkarten

IBM S/390 und zSeries unterstützen hotplugfähige Netzwerkkarten. Die automatische Konfiguration mit DHCP wie bei PC-Netzwerkkarten wird nicht unterstützt. Eine erkannte Netzwerkkarte muss immer noch manuell konfiguriert werden.

Hinweis

21.4.2 Netzwerkkarte konfigurieren mit YaST

Nach Aufruf des YaST Moduls gelangen Sie in eine Übersicht zur Netzwerkkonfiguration. Im oberen Teil des Dialogs werden alle zu konfigurierenden Netzwerkkarten aufgelistet. Falls Ihre Karte beim Start des Systems korrekt erkannt wurde, wird sie hier namentlich aufgeführt. Nicht erkannte Geräte erscheinen als 'Andere (nicht erkannte)'. Im unteren Teil der Ansicht werden bereits konfigurierte Geräte samt Netzwerktyp und Adresse aufgeführt. Sie können nun entweder neue Netzwerkkarten konfigurieren oder die Konfiguration eines bereits konfigurierten Geräts ändern.

Manuelle Konfiguration der Netzwerkkarte

Zur Konfiguration einer nicht erkannten Netzwerkkarte nehmen Sie folgende Grundeinstellungen vor:

Netzwerkschnittstelle Legen Sie den Typ des Netzwerks und die Gerätenummer fest.

Einstellungen für Funkverbindungen
Wenn Sie sich in einem kabellosen Netzwerk befinden (engl. *wireless LAN*) und Ihre Netzwerkkarte für diesen Verbindungstyp ausgelegt ist, gelangen Sie über den Button 'Einstellungen für Funkverbindungen' in den Dialog 'Konfiguration der drahtlosen Netzwerkkarte', in dem Sie Betriebsmodus, Netzwerknamen (ESSID), Netzwerkerkennung (NWID), Verschlüsselung und Spitzname (engl. *nickname*) konfigurieren. Mit 'OK' schließen Sie die Konfiguration Ihrer Karte ab.

► **S/390, zSeries**
Wireless LAN wird auf IBM S/390 und zSeries nicht unterstützt. ◄

Kernelmodul und Auswahl der Netzwerkkarte

Handelt es sich bei Ihrer Netzwerkkarte um ein PCMCIA- oder USB-Gerät, aktivieren Sie die entsprechenden Checkboxen und verlassen diesen Dialog mit 'Weiter'. Andernfalls wählen Sie über den Button 'Auswahl aus Liste' das Modell Ihrer Netzwerkkarte aus. YaST wählt dann automatisch das passende Kernelmodul aus. Verlassen Sie diesen Dialog mit 'Weiter'.

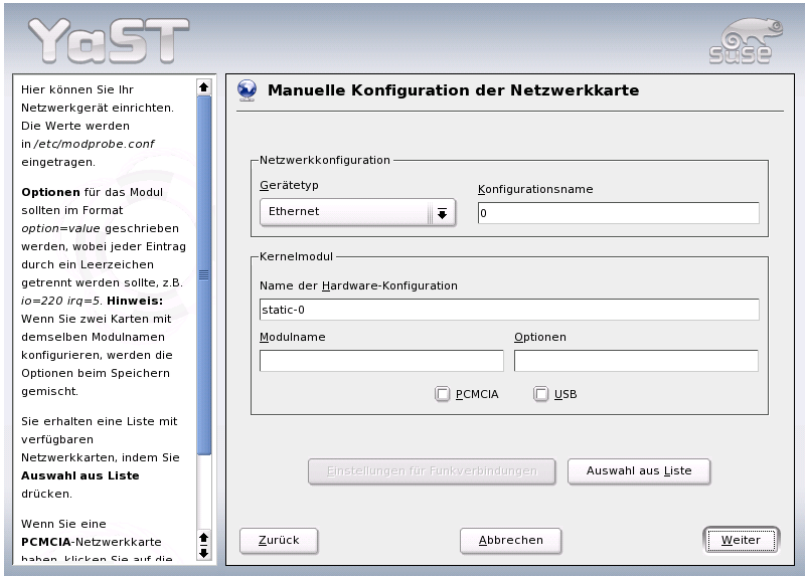

Abbildung 21.3: Konfiguration der Netzwerkkarte

Konfiguration der Netzwerkadresse

Legen Sie die Art der Adressvergabe für Ihre Netzwerkkarte fest:

'Automatische Adressvergabe (mit DHCP)'

Befindet sich ein DHCP-Server innerhalb Ihres Netzes, können Sie sich von dort automatisch die Konfigurationsdaten Ihrer Netzwerkkarte übermitteln lassen. Die Adressvergabe mit DHCP aktivieren Sie ebenfalls, wenn Ihr DSL-Provider Ihnen keine statische IP-Adresse für Ihr System mitgeteilt hat. Bei Verwendung von DHCP gelangen

Sie über die Schaltfläche 'DHCP Client Optionen' zur Client-Konfiguration. Hier stellen Sie ein, ob der DHCP-Server immer auf einen Broadcast antworten soll. Außerdem können Sie optional einen Identifikator angeben. Standardmäßig wird der Rechner anhand der Hardware-Adresse der Netzwerkkarte identifiziert. Benutzen Sie aber mehrere virtuelle Maschinen, die dieselbe Netzwerkarte verwenden, können Sie diese über verschiedene Identifikatoren unterscheiden.

► **S/390, zSeries**
DHCP-Adresskonfiguration wird auf IBM S/390 und zSeries nur auf Netzwerkkarten mit MAC-Adresse unterstützt. Dies sind die Karten des Typs OSA und OSA Express. ◄

'Konfiguration der statischen Addresse'
Verfügen Sie über eine feste IP-Adresse, aktivieren Sie die Checkbox. Geben Sie die IP-Adresse und die für Ihr Netz passende Subnetzmaske ein. Die Voreinstellung für die Subnetzmaske ist so gewählt, dass sie für ein typisches Heimnetz ausreicht.

Sie können diesen Dialog mit 'Weiter' verlassen oder alternativ Rechnernamen, Name-Server und Routing konfigurieren (vgl. Abschnitt 2.6.2 auf Seite 98 und Abschnitt 2.6.7 auf Seite 100).

Kabelmodem

Hinweis

S/390, zSeries: Kabelmodem

Diese Art der Konfiguration wird auf IBM S/390 und zSeries nicht unterstützt.

Hinweis

In manchen Ländern (Österreich, USA) ist der Internetzugang über das Fernsehkabelnetz weit verbreitet. Der Telekabel-Teilnehmer bekommt von der Kabelfirma ein Modem, das einerseits an das Fernsehkabel, andererseits mittels 10Base-T (Twisted-Pair) Leitung an eine Netzwerkkarte im Computer angeschlossen wird. Dieses Modem stellt dann für den Computer eine Standleitung mit einer fixen IP-Adresse dar.

Nach den Angaben Ihres Providers wählen Sie bei der Konfiguration Ihrer Netzwerkkarte zwischen 'Automatische Adressvergabe (mit DHCP)' und 'Konfiguration der statischen Adresse'. Die meisten Provider verwenden

heute DHCP. Eine statische IP-Adresse wird im Allgemeinen bei Business-Paketen der Provider verwendet. Der Provider hat Ihnen in diesem Fall eine feste IP-Adresse zugeteilt.

Lesen Sie dazu unbedingt die Supportdatenbank-Artikel über Einrichtung und Konfigurationen für Kabelmodems, die Sie auch online unter `http://sdb.suse.de/de/sdb/html/cmodem8.html` und `http://sdb.suse.de/en/sdb/html/cmodem8.html` erhalten können.

21.4.3 S/390; zSeries: Netzwerkkonfiguration mit YaST

Konfiguration der qeth-hsi Schnittstelle

Um dem installierten System eine Netzwerkschnittstelle vom Typ `qeth-hsi` (IBM Hipersocket) hinzuzufügen, starten Sie das YaST Netzwerk-Modul ('Netzwerkgeräte' → 'Netzwerkkarte'). Wählen Sie aus der Liste der erkannten Schnittstellen eine der mit 'IBM Hipersocket' bezeichneten Schnittstellen aus, die Sie später für die READ-Geräteadresse verwenden wollen. Klicken Sie auf 'Konfigurieren'. Im Dialog 'Konfiguration der Netzwerkadresse' legen Sie IP-Adresse und Netzmaske für diese Schnittstelle fest. Verlassen Sie die Konfiguration mit 'Weiter' und 'Beenden'.

Konfiguration der qeth-ethernet Schnittstelle

Um dem installierten System eine Netzwerkschnittstelle vom Typ `qeth-ethernet` (IBM OSA Express Ethernet Card) hinzuzufügen, starten Sie das YaST Netzwerk-Modul ('Netzwerkgeräte' → 'Netzwerkkarte'). Wählen Sie aus der Liste der erkannten Schnittstellen eine der mit 'IBM OSA Express Ethernet Card' bezeichneten Schnittstellen aus und klicken Sie auf 'Konfigurieren'. Geben Sie den benötigten Portnamen, einige zusätzliche Optionen (nachzulesen im Handbuch *Linux for zSeries and S/390: Device Drivers, Features, and Commands* von IBM), Ihre IP-Adresse und eine geeignete Netzmaske an. Verlassen Sie die Konfiguration mit 'Weiter' und 'Beenden'.

Konfiguration der ctc Schnittstelle

Um dem installierten System eine Netzwerkschnittstelle vom Typ `ctc` (IBM parallel CTC Adapter) hinzuzufügen, starten Sie das YaST Netzwerk-Modul ('Netzwerkgeräte' → 'Netzwerkkarte'). Wählen Sie aus der Liste der erkannten Schnittstellen eine der mit 'IBM parallel CTC Adapter' bezeichneten Schnittstellen aus, die Sie später für den READ Kanal verwenden wollen. Klicken Sie auf 'Konfigurieren'. Wählen Sie im nächsten Dialog

per Drop-Down Menü in den 'Einstellungen für S/390 Devices' den geeigneten Betriebsmodus (meist 'Kompatibilitätsmodus') für die Schnittstelle aus und spezifizieren Sie IP-Adresse der Schnittstelle und die IP-Adresse des Peers. Wenn nötig, passen Sie die MTU-Größe an ('Erweitert' → 'Besondere Einstellungen'). Verlassen Sie die Netzwerkkonfiguration mit 'Weiter' und 'Beenden'.

Konfiguration der lcs Schnittstelle

Um dem installierten System eine Netzwerkschnittstelle vom Typ `lcs` (IBM OSA-2 Adapter) hinzuzufügen, starten Sie das YaST Netzwerk-Modul ('Netzwerkgeräte' → 'Netzwerkkarte'). Wählen Sie aus der Liste der erkannten Schnittstellen eine der mit 'IBM OSA-2 Adapter' bezeichneten Schnittstellen aus und klicken Sie auf 'Konfigurieren'. Geben Sie die benötigte Portnummer, einige zusätzliche Optionen (nachzulesen im Handbuch *Linux for zSeries and S/390: Device Drivers, Features, and Commands* von IBM), Ihre IP-Adresse und eine geeignete Netzmaske an. Verlassen Sie die Konfiguration mit 'Weiter' und 'Beenden'.

Konfiguration der IUVC Schnittstelle

Um dem installierten System eine Netzwerkschnittstelle vom Typ `iucv` (IUCV) hinzuzufügen, starten Sie das YaST Netzwerk-Modul ('Netzwerkgeräte' → 'Netzwerkkarte'). Wählen Sie aus der Liste der erkannten Schnittstellen eine mit 'IUCV' bezeichnete aus. Klicken Sie auf 'Konfigurieren'. YaST fragt nun nach dem Namen Ihres IUCV-Partners. Geben Sie diesen Namen ein und beachten Sie Groß- und Kleinschreibung. Klicken Sie auf 'Weiter'. Geben Sie Ihre IP-Adresse und die Ihres IUCV-Partners ein. Wenn nötig, passen Sie die MTU-Größe an ('Erweitert' → 'Besondere Einstellungen'). Verlassen Sie die Netzwerkkonfiguration mit 'Weiter' und 'Beenden'.

21.4.4 Modem

Hinweis

S/390, zSeries: Modem

Diese Art der Konfiguration wird auf IBM S/390 und zSeries nicht unterstützt.

Hinweis

Im YaST-Kontrollzentrum finden Sie unter ‘Netzwerkgeräte’ die Modem-Konfiguration. Falls die automatische Erkennung fehlschlägt, wählen Sie die manuelle Konfiguration. In dem sich öffnenden Dialog ist bei ‘Modemgerät’ die Schnittstelle einzutragen.

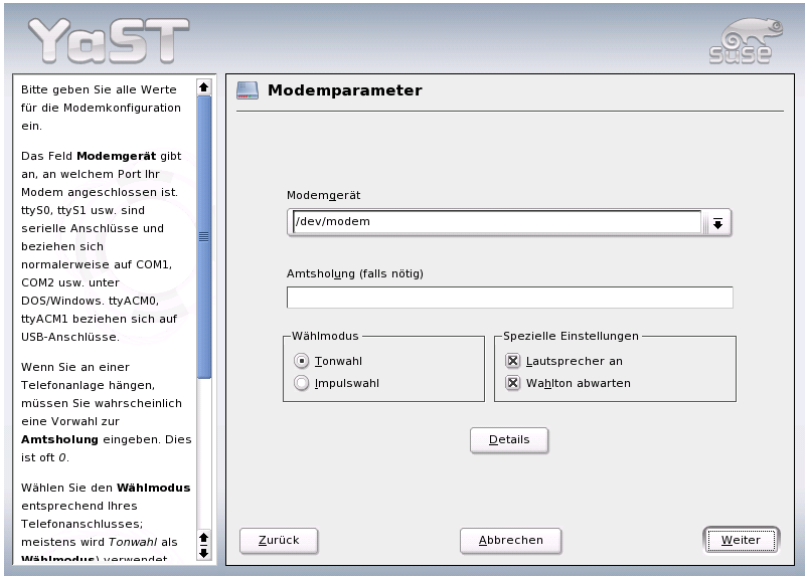

Abbildung 21.4: *Modemkonfiguration*

Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie gegebenenfalls die Vorwahl für die Amtsholung eintragen (normalerweise eine Null; dies erfahren Sie in der Bedienungsanleitung Ihrer Telefonanlage). Zudem können Sie sich zwischen Ton- und Impulswahl entscheiden; zusätzlich auch, ob der Lautsprecher angeschaltet ist oder ob der Wahlton abgewartet werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Unter ‘Details’ finden Sie Einstellungen zur Baudrate und Initialisierungs-Strings für das Modem. Hier sollten Sie nur dann Änderungen vornehmen, wenn Ihr Modem nicht automatisch erkannt wurde und für die Datenübertragung speziell eingestellt werden muss. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Verlassen Sie den Dialog mit ‘OK’.

Wählen Sie im folgenden Dialog den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste für Ihr Land voreingestellter Provider

auswählen wollen, aktivieren Sie den Radiobutton 'Länder'. Alternativ gelangen Sie über den Button 'Neu' in den Dialog zur manuellen Festlegung der ISP-Parameter. Dort geben Sie den Namen der Einwahl und des Providers und dessen Telefonnummer ein. Außerdem tragen Sie hier den Benutzernamen und das Passwort ein, das Ihnen Ihr Provider für die Einwahl zur Verfügung gestellt hat. Aktivieren Sie die Checkbox 'Passwortabfrage', wenn Sie bei jeder Einwahl nach dem Passwort gefragt werden wollen.

Im letzten Dialog geben Sie die Verbindungsparameter ein:

'Dial-On-Demand' Geben Sie mindestens einen Name-Server an, wenn Sie Dial-on-demand verwenden wollen.

'Während Verbindung DNS ändern'
Standardmäßig ist diese Checkbox aktiviert, der Name-Server wird also bei jeder Einwahl ins Internet automatisch angepasst. Deaktivieren Sie diese Einstellung und setzen Sie feste Name-Server, wenn Sie sich für 'Automatische Einwahl' entscheiden.

'Ignoranz-Modus' Diese Option ist standardmäßig aktiviert. Eingabeaufforderungen vom Einwahl-Server werden ignoriert, um den Verbindungsaufbau zu erleichtern.

'Firewall aktivieren' Hiermit schalten Sie die SUSE Firewall ein und sind sicher gegen Eindringlinge geschützt, während Sie mit dem Internet verbunden sind.

'Abbrechen nach (Sekunden)' Sie können bestimmen, nach welcher Zeit die Verbindung abgebrochen werden soll, wenn kein Informationsfluss mehr stattfindet .

IP-Details Über diesen Button gelangen Sie in den Dialog zur Adresskonfiguration. Sollte Ihnen Ihr Provider keine dynamische IP-Adresse zur Verfügung gestellt haben, deaktivieren Sie die Checkbox 'Dynamische IP-Adresse' und tragen Sie die lokale IP-Adresse Ihres Rechners und die entfernte IP-Adresse ein. Beide Angaben können Sie von Ihrem Provider erfragen. Belassen Sie die Einstellung zur 'Standard-Route' im aktivierten Zustand und verlassen den Dialog mit 'OK'.

Mit 'Weiter' landen Sie wieder im Übersichtsdialog und sehen, was Sie konfiguriert haben. Schließen Sie die Einrichtung mit 'Beenden' ab.

21.4.5 DSL

Hinweis

S/390, zSeries: DSL

Diese Art der Konfiguration wird auf IBM S/390 und zSeries nicht unterstützt.

Hinweis

Zur Konfiguration von DSL dient das YaST-Modul 'DSL' unter der Rubrik 'Netzwerkgeräte'. In mehreren Dialogen haben Sie hier die Möglichkeit, die Kenndaten Ihres DSL-Zugangs einzugeben. Mit YaST können Sie DSL-Zugänge einrichten, die auf den folgenden Protokollen aufsetzen:

- PPP über Ethernet (PPPoE) - Deutschland
- PPP über ATM (PPPoATM) - England
- CAPI für ADSL (Fritz-Karten)
- Tunnelprotokoll für Point-to-Point (PPTP) - Österreich

Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration Ihrer Netzwerkkarte voraussetzt. Falls dies nicht schon geschehen ist, kommen Sie mit 'Netzwerkkarten konfigurieren' direkt zum entsprechenden Dialog (siehe Abschnitt 21.4.2 auf Seite 482). Die automatische IP-Adressenvergabe findet bei DSL nicht mit dem DHCP-Protokoll statt. Deshalb dürfen Sie auch nicht 'Automatische Adressvergabe (mit DHCP)' verwenden. Vergeben Sie stattdessen bitte eine statische Dummy-IP-Adresse wie z.B. `192.168.22.1`. Im Feld 'Subnetzmaske' ist der Wert `255.255.255.0` einzutragen. Bitte achten Sie unbedingt darauf, dass Sie für ein Einzelplatzsystem keinen Eintrag in das Feld 'Standardgateway' machen.

Hinweis

Die Werte für 'IP-Adresse' Ihres Rechners und 'Subnetzmaske' sind nur Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Aktivierung der Netzwerkkarte benötigt.

Hinweis

Zu Beginn der Konfiguration (siehe Abb. 21.5 auf der nächsten Seite) wählen sie bitte den PPP-Modus und jene Ethernetkarte aus, an die Ihr Modem

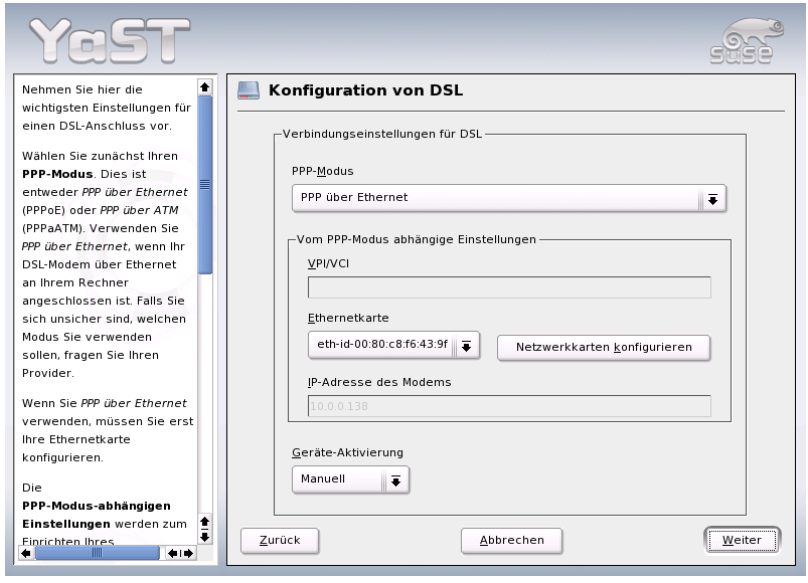

Abbildung 21.5: *DSL-Konfiguration*

angeschlossen ist (in der Regel ist dies `eth0`). Mit der Kombobox 'Geräte-Aktivierung' können Sie bestimmen, ob die DSL-Verbindung schon beim Booten des Systems oder erst später, z.B. manuell hergestellt werden soll. Im weiteren Verlauf können Sie dann Ihr Land und den dort ansässigen Dienstanbieter (Provider) auswählen. Die Inhalte der danach folgenden Dialoge hängen stark von den vorher gewählten Einstellungen ab und werden hier daher nur kurz angesprochen. Wenn einzelne Optionen unklar sind, lesen Sie bitte die ausführlichen Hilfetexte zu den Dialogen.

Um 'Dial-On-Demand' nutzen zu können, müssen Sie bei Einzelplatzsystemen auf jeden Fall DNS (Name-Server) konfigurieren. Die meisten Provider unterstützen heute dynamische DNS-Vergabe, das heißt, beim Verbindungsaufbau wird eine aktuelle IP-Adresse des Name-Servers übergeben. Dennoch muss in Ihrem Einzelplatzsystem in diesem Dialog ein Platzhalter für einen DNS-Server eingetragen werden z.B. `192.168.22.99`. Falls Sie keine dynamische Zuweisung des Name-Servers bekommen, müssen Sie hier die IP-Adressen der Name-Server Ihres Providers eintragen.

Interessant ist auch die Kombobox 'Verbindung abbrechen nach (Sekunden)'. Hier können Sie einstellen, wie lange die Verbindung nach dem letz-

ten Datentransfer aufrecht erhalten bleibt, bevor sie automatisch abgebaut wird. Werte zwischen 60 und 300 Sekunden sind hier empfehlenswert.

Hinweis

Dial-On-Demand

Bei 'Dial-On-Demand' wird die Verbindung nach Verstreichen dieser Wartezeit nicht komplett abgebaut, sondern verbleibt in einem Wartezustand, der einen automatischen Wiederaufbau ermöglicht, sobald Daten übertragen werden müssen. Wird 'Dial-On-Demand' nicht verwendet, erfolgt ein echter Verbindungsabbau, so dass vor einer erneuten Übertragung die Verbindung manuell wiederhergestellt werden muss. Sie können für diesen Fall den automatischen Verbindungsabbau unterbinden, wenn Sie die Wartezeit auf 0 Sekunden setzen.

Hinweis

Zur Konfiguration von T-DSL verfahren Sie ähnlich wie bei DSL. Durch Auswahl von 'T-Online' als Provider gelangen Sie automatisch in den Konfigurationsdialog für T-DSL. Sie benötigen dafür noch zusätzlich folgende Daten: Anschlusskennung, T-Online-Nummer, Mitbenutzerkennung und Ihr persönliches Kennwort. Entnehmen Sie diese Informationen bitte Ihren T-DSL-Anmeldeunterlagen.

21.4.6 ISDN

Hinweis

S/390, zSeries: ISDN

Diese Art der Konfiguration wird auf IBM S/390 und zSeries nicht unterstützt.

Hinweis

Dieses Modul erlaubt die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn Ihre ISDN-Karte von YaST nicht automatisch erkannt wurde, müssen Sie die Karte zunächst auswählen. Theoretisch können Sie mehrere Interfaces einrichten, im Normalfall ist dies für den Heimanwender aber nicht notwendig, da er für ein Interface mehrere Provider einrichten kann. Die nachfolgenden Dialoge dienen dann der Einstellung der verschiedenen ISDN-Parameter für den Betrieb der Karte.

Der nächste Dialog (vgl. Abb. 21.7 auf Seite 493) erlaubt die 'Auswahl des ISDN-Protokolls'. Der Standard ist hier 'Euro-ISDN (EDSS1)' (vgl. unten

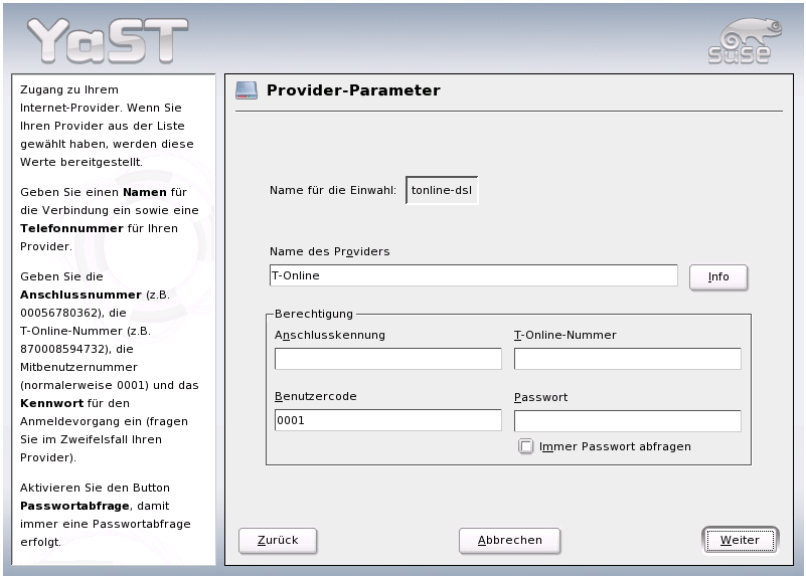

Abbildung 21.6: *T-DSL-Konfiguration in Deutschland*

Fall 1. und 2.a), für ältere bzw. große Telefonanlagen (vgl. unten Fall 2.b) verwenden Sie '1TR6'. Für die USA gilt 'NI1'. Die Landeskennung können Sie in der entsprechenden Auswahlbox aussuchen. Im Eingabefeld daneben wird dann die richtige Vorwahl (z.B. +49 für Deutschland) eingetragen. Zusätzlich müssen Sie noch die Ortskennziffer (Vorwahl) Ihres Standortes im Feld 'Ortskennziffer' eingeben (z.B. 911 für Nürnberg). Falls nötig, tragen Sie hier außerdem die Amtsholung ein.

Die Auswahlbox 'Startmodus' erlaubt die Einstellung des Startmodus für die aktuelle ISDN-Karte. 'OnBoot' bewirkt, dass der ISDN-Treiber jeweils beim Systemstart initialisiert wird. Entscheiden Sie sich hier für 'Manuell', muss der ISDN-Treiber per Hand durch den Benutzer `root` mit `rcisdn start` initialisiert werden. Die Option 'Hotplug' lädt den Treiber beim Anschließen der PCMCIA-Karte oder des USB-Geräts. Nachdem Sie alle Einstellungen vorgenommen haben, klicken Sie auf 'OK'.

Im nächsten Dialog können Sie die Schnittstelle für Ihre ISDN-Karte definieren oder weitere Provider zu bestehenden Schnittstellen hinzufügen. Die Schnittstellen können in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die meisten Internet-Provider verwenden den Modus

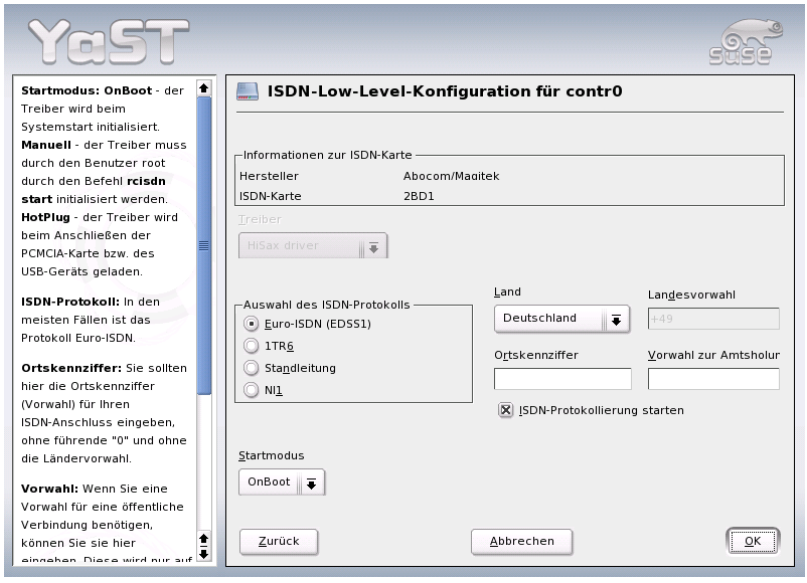

Abbildung 21.7: *ISDN-Konfiguration*

SyncPPP, der nachfolgend beschrieben wird.

Für die Angabe 'Eigene Telefonnummer' müssen Sie je nach Anschlussszenario eine der folgenden Angaben machen:

1. **ISDN-Karte direkt an der Telefondose (NTBA)**

   ISDN bietet Ihnen standardmäßig drei Rufnummern (MSN *Multiple Subscriber Number*), auf Wunsch bis zu zehn, welche für Ihren Anschluss zur Verfügung gestellt werden. An dieser Stelle müssen Sie eine der MSN-Nummern Ihrer ISDN-Karte zuweisen. Die Angabe der Nummer erfolgt ohne Angabe der Vorwahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

2. **ISDN-Karte an einer Telefonanlage**

   Je nach Anwendungsfall sind verschiedene Angaben notwendig.

   (a) für den Hausgebrauch: In der Regel wird bei kleinen Telefonanlagen als Protokoll Euro-ISDN/EDSS1 für die internen Anschlüsse verwendet. Diese Telefonanlagen haben einen internen

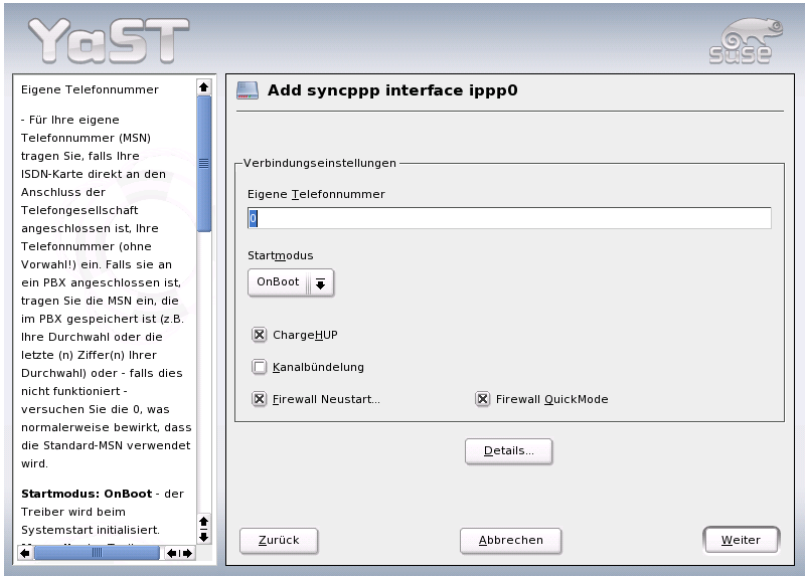

Abbildung 21.8: *ISDN-Schnittstellenkonfiguration*

S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

(b) für Firmen: Normalerweise wird bei großen Telefonanlagen als Protokoll 1TR6 für die internen Anschlüsse verwendet. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Linux-Konfiguration ist normalerweise nur die letzte Ziffer der EAZ einzutragen. Im Notfall probieren Sie die Ziffern 1 bis 9.

Per Checkbox legen Sie fest, ob Sie eine automatische Beendigung bestehender Verbindungen vor der nächsten zu zahlenden Gebühreneinheit wünschen ('ChargeHUP'). Beachten Sie in diesem Zusammenhang, dass dies unter Umständen noch nicht mit jedem Provider funktioniert. Wün-

schen Sie eine 'Kanalbündelung' (Multilink PPP), aktivieren Sie die entsprechende Checkbox. Soll die SuSEfirewall2 gestartet werden, wählen Sie die Checkbox 'Firewall aktivieren' an.

Über den Button 'Details' gelangen Sie in einen Dialog, der für die Umsetzung komplexerer Anschlussszenarien ausgelegt ist. Für normale Heimanwender ist dieser Dialog nicht relevant. Sie verlassen den Dialog mit 'Weiter'.

Im nächsten Dialog treffen Sie die Einstellungen für die Vergabe der IP-Adressen. Hat Ihr Provider Ihnen keine statische IP-Adresse zugewiesen, wählen Sie 'Dynamische IP-Adresse'. Andernfalls tragen Sie in die entsprechenden Felder nach den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse ein. Soll das anzulegende Interface als Standardroute ins Internet dienen, aktivieren Sie die Checkbox 'Standardroute'. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standardroute in Frage kommt. Verlassen Sie diesen Dialog mit 'Weiter'.

Im nachfolgenden Dialog bestimmen Sie Ihr Land und Ihren Provider. Bei den aufgelisteten Anbietern handelt es sich um Call-by-Call-Provider. Wollen Sie einen Provider verwenden, welcher nicht in dieser Liste aufgeführt ist, so klicken Sie auf 'Neu'. Es erscheint die Maske 'ISP-Parameter', in der Sie alle notwendigen Einstellungen bezüglich Ihres gewünschten Providers vornehmen können. Die Telefonnummer darf keinerlei Trennung wie Komma oder Leerzeichen enthalten. Weiter geben Sie den Benutzernamen und das Passwort ein, welche Sie von Ihrem Provider erhalten haben. Klicken Sie danach auf 'Weiter'.

Um 'Dial on demand' nutzen zu können, müssen Sie bei Einzelplatzsystemen auf jeden Fall DNS (Name-Server) konfigurieren. Die meisten Provider unterstützen heute dynamische DNS-Vergabe, das heißt beim Verbindungsaufbau wird eine aktuelle IP-Adresse des Name-Servers übergeben. Dennoch muss in Ihrem Einzelplatzsystem in diesem Dialog ein Platzhalter für einen DNS-Server eingetragen werden wie z. B. `192.168.22.99`. Falls Sie keine dynamische Zuweisung des Name-Servers bekommen, müssen Sie hier die IP-Adressen der Name-Server Ihres Providers eintragen. Ferner können Sie einstellen, nach wie vielen Sekunden die Verbindung automatisch abgebrochen werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Schließlich bestätigen Sie Ihre Einstellungen mit 'Weiter' und gelangen in eine Übersicht der konfigurierten Schnittstellen. Aktivieren Sie Ihre Einstellungen schließlich mit 'Beenden'.

21.4.7 Hotplug/PCMCIA

Hinweis

S/390, zSeries: Hotplug-Unterstützung

Unter IBM S/390 und zSeries werden alle Netzwerkkarten über Hotplug erkannt und hochgefahren.

Hinweis

Eine Sonderstellung nehmen hotplugfähige Netzwerkkarten ein wie zum Beispiel PCMCIA- oder USB-Geräte. Im Gegensatz zu fest eingebauten Netzwerkkarten, die eine gleich bleibende Gerätebezeichnung erhalten, beispielsweise `eth0`, wird solchen Karten dynamisch bei Bedarf eine freie Gerätebezeichnung zugewiesen. Um Konflikte mit eventuell fest eingebauten Karten zu vermeiden wird PCMCIA und Hotplug beim Booten erst nach dem Netzwerk gestartet.

Diese Karten werden automatisch eingerichtet sobald sie eingesetzt bzw. beim Booten erkannt werden. Deshalb ist es nicht notwendig, dass PCMCIA vor dem Netzwerk gestartet wird. Im Gegenteil: Wenn diese Karten nur vom Netzwerkstartscript beim Booten behandelt würden, ginge die Möglichkeit, sie zur Laufzeit des Systems zu tauschen, verloren.

21.4.8 Konfiguration von IPv6

Hinweis

S/390, zSeries: IPv6-Unterstützung

CTC- und IUCV- Netzwerkschnittstellen unterstützen kein IPv6.

Hinweis

Falls Sie die Verwendung von IPv6 konfigurieren möchten, müssen Sie in der Regel keine Konfiguration auf den Arbeitsstationen durchführen. Allerdings muss die IPv6-Unterstützung geladen werden. Rufen Sie als Benutzer `root` den Befehl `modprobe ipv6` auf.

Aufgrund der Autokonfigurationsphilosophie von IPv6 wird dann der Netzwerkkarte eine Adresse im `link-local` Netz zugewiesen. Normalerweise wird auf einer Arbeitsstation keine Routingtabelle gepflegt. Die Router im Netz können über das Router Advertisment Protocol von der Arbeitsstation darüber befragt werden, welches Präfix und welche Gateways zu verwenden sind. Um einen IPv6-Router aufzusetzen, können Sie das

Programm radvd aus `radvd` verwenden. Dieses Programm teilt den Arbeitsstationen das zu verwendende Präfix für IPv6-Adressen und den/die Router mit. Das Programm zebra kann ebenfalls zur Autokonfiguration von Adressen und für Routingkonfiguration eingesetzt werden.

Um einer Arbeitsstation eine IPv6-Adresse zuweisen zu können, ist es ratsam, einen Router mit dem Programm radvd oder zebra zu installieren und zu konfigurieren. Die Arbeitsstationen bekommen die IPv6-Adresse dann automatisch zugewiesen.

Zur Einrichtung verschiedener Tunnel mit Hilfe der Dateien unter `/etc/sysconfig/network` finden Sie wichtige Informationen in der Manualpage von ifup (`man ifup`).

21.5 Routing unter SuSE Linux

Ab SUSE LINUX 8.0 wird die Routing-Tabelle in den Konfigurationsdateien `/etc/sysconfig/network/routes` und `/etc/sysconfig/network/ifroute-*` eingestellt.

In der Datei `/etc/sysconfig/network/routes` können alle statischen Routen eingetragen werden, die für die verschiedenen Aufgaben eines Systems benötigt werden könnten: Route zu einem Rechner, Route zu einem Rechner über ein Gateway und Route zu einem Netzwerk. Hier wird z.B. der Default Gateway bei statischen Routen konfiguriert:

```
default GATEWAY - -
```

wobei GATEWAY die IP-Adresse des Gateways ist.

Für alle Interfaces, die individuelles Routing benötigen, kann dies jeweils in einer eigenen Datei pro Interface definiert werden: `/etc/sysconfig/network/ifroute-*`. Für das Zeichen * muss die Interface-Bezeichnung eingesetzt werden. Die Einträge können folgendermaßen aussehen:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

Falls GATEWAY, NETMASK, PREFIXLEN oder INTERFACE nicht angegeben werden, muss an ihrer Stelle das Zeichen - gesetzt werden. Die Einträge TYPE und OPTIONS können schlicht entfallen.

- In der ersten Spalte steht das Ziel einer Route. Dabei kann dort die IP-Adresse eines Netzes oder Rechners oder bei *erreichbaren* Nameservern auch der voll qualifizierte Name eines Netzes oder eines Rechners stehen.
- Die zweite Spalte enthält entweder das Default-Gateway oder ein Gateway, hinter dem ein Rechner oder Netzwerk erreichbar ist.
- Die dritte Spalte enthält die Netzmaske für Netzwerke oder Rechner hinter einem Gateway. Für Rechner hinter einem Gateway lautet die Maske zum Beispiel `255.255.255.255`.
- Die letzte Spalte ist nur für die am lokalen Rechner angeschlossenen Netzwerke (Loopback, Ethernet, ISDN, PPP, ...) wichtig. Hier muss der Name des Devices eingetragen werden.

21.6 SLP — Dienste im Netz vermitteln

Das *Service Location Protocol* (kurz: SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerkes zu vereinfachen. Um einen Netzwerkclient inklusive aller gewünschten Dienste zu konfigurieren, braucht sein Administrator traditionell detailliertes Wissen über die in seinem Netz verfügbaren Server. Mit SLP wird die Verfügbarkeit eines bestimmten Dienstyps allen Clients im lokalen Netz bekanntgegeben. Anwendungen, die SLP unterstützen, können die per SLP verteilte Information nutzen und sind damit automatisch konfigurierbar.

Hinweis

SLP-Unterstützung in SUSE LINUX Enterprise Server

Unter anderem bieten folgenden Dienste SLP-Unterstützung: cupsd, rsyncd, ypserv, openldap2, openwbem (CIM), ksysguardd, saned, kdm vnc login, smpppd, rpasswd, postfix, sshd (via fish.)

Hinweis

21.6.1 SLP-Unterstützung in SUSE LINUX

SUSE LINUX unterstützt die Installtion von per SLP vermittelten Installationsquellen und enthält viele Systemdienste mit integrierter Unterstützung

für SLP. YaST und Konqueror verfügen beide über entsprechende Frontends für SLP. Nutzen Sie SLP, um zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem SUSE LINUX Enterprise Server den vernetzten Clients zur Verfügung zu stellen.

Installation per SLP

Bieten Sie innerhalb Ihres Netzwerks einen Installationsserver mit SUSE LINUX Installationsmedien an, kann dieser SLP-registriert werden (Details siehe Abschnitt 4.1 auf Seite 166). Wird SLP-Installation gewählt, startet linuxrc nach dem Boot vom gewählten Bootmedium eine SLP-Anfrage und bietet die gefundenen Quellen zur Auswahl.

Eigene Dienste registrieren

Viele Applikationen unter SUSE LINUX verfügen bereits über integrierte SLP-Unterstützung durch die Nutzung der `libslp`-Bibliothek. Möchten Sie darüber hinaus weitere Dienste über SLP verfügbar machen, die keine SLP-Unterstützung einkompiliert haben, stehen Ihnen mehrere Möglichkeiten offen:

Statische Registrierung über `/etc/slp.reg.d/`
Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Ein Beispiel einer solchen Datei für die Registrierung eines Scanner-Dienstes folgt:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die so genannte *Service-URL*, die mit `service:` eingeleitet wird. Sie enthält den Diensttyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. ⟨*$HOSTNAME*⟩ wird automatisch durch den vollständigen Hostnamen ersetzt. Durch einen Doppelpunkt getrennt, folgt nun der TCP-Port, auf dem der betroffene Dienst lauscht. Geben Sie von der Service-URL durch Kommata abgetrennt nun noch die Sprache an, in der sich der Dienst ankündigen soll und die Lebensdauer der Registrierung in Sekunden. Der Wert für die Lebensdauer der Registrierung kann zwischen `0` und `65535` annehmen. Mit `0`

wäre die Registrierung unwirksam, mit `65535` wird sie nicht eingeschränkt.

Die Registrierungsdatei enthält ausserdem die beiden Variablen `watch-tcp-port` und `description` enthalten. Erstere koppelt die SLP-Ankündigung des Dienstes daran, ob der slpd den Status des Dienstes überprüft. Die letzte Variable enthält eine genauere Beschreibung des Dienstes, die in geeigneten Browsern angezeigt wird.

Hinweis

YaST und SLP

Einige von YaST vermittelten Dienste wie 'Installationsserver' oder 'YOU-Server' nehmen diese Registrierung automatisch für Sie vor, wenn Sie die SLP-Checkboxen in den Moduldialogen aktivieren. YaST legt dann für diese Dienste Registrierungsdateien an.

Hinweis

Statische Registrierung `/etc/slp.reg`
Einziger Unterschied zu dem oben beschriebenen Verfahren ist die Bündelung aller Dienste innerhalb einer zentralen Datei.

Dynamische Registrierung mit slptool
Soll aus eigenen Skripten ein SLP-Registrierung eines Dienstes erfolgen, nutzen Sie das Kommandozeilen-Frontend slptool.

SLP-Frontends in SUSE LINUX

SUSE LINUX enthält mehrere Frontends, um SLP-Informationen über ein Netzwerk abzufragen und weiterzuverwenden:

slptool slptool ist ein einfaches Kommandozeilenprogramm, das verwendet werden kann, um SLP-Anfragen im Netz bekanntzugeben oder auch, um eigene Dienste anzukündigen. `slptool --help` listet alle verfügbaren Optionen und Funktionen. slptool kann auch aus Skripten heraus aufgerufen werden, die SLP-Informationen verarbeiten sollen.

YaST SLP-Browser YaST enthält unter 'Netzwerkdienste' → 'SLP-Browser' einen eigenen SLP-Browser, der in einer grafischen Baumansicht alle in lokalen Netz per SLP angekündigten Dienste auflistet.

Konqueror Als Netzwerkbrowser eingesetzt, kann Konqueror mit dem Aufruf `slp:/` alle im lokalen Netz verfügbaren SLP-Dienste anzeigen. Mit einem Klick auf die im Hauptfenster angezeigten Icons erhalten Sie genauere Informationen über den genannten Dienst.

Rufen Sie Konqueror mit `service:/` auf, löst ein Klick auf das entsprechende Icon im Browserfenster einen Verbindungsaufbau zum gewählten Dienst aus.

SLP aktivieren

Hinweis

Aktivierung des slpd

Der slpd muss auf Ihrem System laufen, sobald Sie eigene Serverdienste anbieten wollen. Für das bloße Abfragen von Diensten ist ein Start dieses Daemons nicht notwendig.

Hinweis

Der slpd Daemon wird wie die meisten Systemdienste unter SUSE LINUX über ein eigenes Init-Skript gesteuert. Standardmäßig ist der Daemon inaktiv. Möchten Sie ihn für die Dauer einer Sitzung aktivieren, verwenden Sie als `root` das Kommando `rcslpd start`, um ihn zu starten und `rcslpd stop`, um ihn zu stoppen. Mit `restart` bzw. `status` lösen Sie einen Neustart bzw. eine Statusabfrage aus. Soll slpd standardmäßig aktiv sein, rufen Sie als `root` einmalig das Kommando `insserv slpd` auf. Damit ist slpd automatisch in die Menge der beim Systemboot zu startenden Dienste aufgenommen.

21.6.2 Weitere Informationen

Für tiefergehende Informationen zum Thema SLP stehen Ihnen folgende Quellen zur Verfügung:

RFC 2608, 2609, 2610 RFC 2608 befasst sich allgemein mit der Definition von SLP. RFC 2609 geht näher auf die Syntax der verwendeten Service-URLs ein und RFC 2610 greift DHCP via SLP auf.

http://www.openslp.com Die Homepage des OpenSLP-Projekts.

file:/usr/share/doc/packages/openslp/* In diesem Verzeichnis finden Sie sämtliche verfügbare Dokumentation zu SLP inklusive eines `README.SuSE` mit den SUSE LINUX

Spezifika, den oben genannten RFCs und zwei einführenden HTML-Dokumenten. Programmierer, die SLP-Funktionen verwenden wollen, sollten das Paket `openslp-devel` installieren, um den mitgelieferten *Programmers Guide* zu nutzen.

21.7 DNS – Domain Name System

DNS (engl. *Domain Name System*) wird benötigt, um die Domain- und Rechnernamen in IP-Adressen aufzulösen. Bevor Sie einen eigenen Nameserver einrichten, sollten Sie die allgemeinen Informationen zu DNS im Abschnitt 21.1.3 auf Seite 461 lesen.

Die folgenden Konfigurationsbeispiele beziehen sich auf BIND 9.

21.7.1 Nameserver BIND starten

Der Nameserver BIND (*Berkeley Internet Name Domain*) ist auf SUSE LINUX bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann. Hat man bereits eine funktionsfähige Internetverbindung und trägt in der `/etc/resolv.conf` als Nameserver `127.0.0.1` für `localhost` ein, hat man in der Regel schon eine funktionierende Namensauflösung, ohne dass man den DNS des Providers kennt. BIND führt so die Namensauflösung über die Root-Nameserver durch, was aber merklich langsamer ist. Normalerweise sollte man den DNS des Providers mit seiner IP-Adresse in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` eintragen, um eine effektive und sichere Namensauflösung zu erhalten. Funktioniert das soweit, läuft der Nameserver als reiner „Caching-only"-Nameserver. Erst wenn man ihm eigene Zonen bereitstellt, wird er ein richtiger DNS werden. Ein einfaches Beispiel dafür, findet man im Dokumentations-Verzeichnis: `/usr/share/doc/packages/bind9/sample-config`.

Man sollte allerdings keine offizielle Domain aufsetzen, solange man diese nicht von der zuständigen Institution — für `.de` ist das die DENIC eG — zugewiesen bekommen hat. Auch wenn man eine eigene Domain hat, diese aber vom Provider verwaltet wird, sollte man diese besser nicht verwenden, da BIND sonst keine Anfragen für diese Domain mehr forwarden (weiterleiten) würde und so zum Beispiel der Webserver beim Provider für die eigene Domain nicht mehr erreichbar wäre.

Um den Nameserver zu starten, gibt man auf der Kommandozeile als `root` ein:

```
rcnamed start
```

Erscheint rechts in grün „done“, ist der `named`, so heißt der Nameserver-Prozess, erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit des Nameservers sofort testen, indem man die Programme `host` oder `dig` verwendet. Als Default-Server muss `localhost` mit der Adresse `127.0.0.1` angezeigt werden. Sollte das nicht der Fall sein, steht wahrscheinlich in der `/etc/resolv.conf` ein falscher Nameserver oder diese Datei existiert gar nicht. Für einen ersten Test gibt man `host 127.0.0.1` ein, das sollte immer funktionieren; erhält man eine Fehlermeldung, sollte man mit folgendem Kommando überprüfen, ob der `named` überhaupt läuft

```
rcnamed status
```

Falls der Nameserver nicht startet oder ein fehlerhaftes Verhalten zeigt, findet man die Ursache in den meisten Fällen in `/var/log/messages` protokolliert.

Um den Nameserver des Providers oder um einen eigenen, der bereits im lokalen Netz läuft, als „Forwarder“ zu verwenden, trägt man diesen oder auch mehrere, im Abschnitt `options` unter `forwarders` ein; die in Datei 21.10 verwendeten IP-Adressen sind willkürlich gewählt und müssen entsprechend den eigenen Gegebenheiten angepasst werden.

Beispiel 21.10: *Forwarding-Optionen in named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

Nach den `options` folgen die Einträge für die Zonen, die Einträge für `localhost`, `0.0.127.in-addr.arpa`, sowie `.` vom `type hint` sollten immer vorhanden sein. Die zugehörigen Dateien müssen nicht verändert werden, da sie so funktionieren wie sie sind. Beachten muss man auch, dass nach jedem Eintrag ein `;` steht und die geschweiften Klammern korrekt gesetzt sind. Hat man nun Änderungen an der Konfigurationsdatei `/etc/named.conf` oder an den Zonen-Dateien vorgenommen, muss man BIND mit dem Kommando `rcnamed reload` dazu veranlassen, diese neu einzulesen. Alternativ kann man den Nameserver auch komplett mit dem Befehl `rcnamed restart` neu starten. Mit dem Kommando `rcnamed stop` kann man den Nameserver jederzeit komplett beenden.

21.7.2 Die Konfigurationsdatei /etc/named.conf

Alle Einstellungen zum Nameserver BIND sind in der Datei `/etc/named.conf` vorzunehmen. Die Zonendaten selbst, die Rechnernamen, IP-Adressen usw. für die zu verwaltenden Domains, sind in separaten Dateien im Verzeichnis `/var/lib/named` abzulegen, dazu aber unten mehr.

Die `/etc/named.conf` unterteilt sich grob in zwei Bereiche, zum einen der Abschnitt `options` für allgemeine Einstellungen und zum anderen die `zone`-Einträge für die einzelnen Domains. Außerdem kann man noch einen Bereich `logging`, sowie Einträge vom Typ `acl` (engl. *Access Control List*) definieren. Kommentarzeilen beginnen mit einem #-Zeichen, alternativ ist `//` auch erlaubt.

Eine minimalistische `/etc/named.conf` stellt Datei 21.11 dar.

Beispiel 21.11: *Minimalistische Datei /etc/named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

Hinweis

Weitere Informationen zur BIND-Konfiguration

Weitere aktuelle Information zur BIND-Konfiguration unter SUSE LINUX erhalten Sie unter `/usr/share/doc/packages/bind/README.SuSE`.

Hinweis

21.7.3 Die wichtigsten Konfigurationsoptionen im Abschnitt options

directory "/var/lib/named"; gibt das Verzeichnis an, in dem der BIND die Dateien mit den Zonendaten findet.

forwarders 10.0.0.1; ; verwendet man, um den oder die Nameserver (meist des Providers) anzugeben, an den oder die die DNS-Anfragen weitergereicht werden, die nicht direkt beantwortet werden können.

forward first; bewirkt, dass die DNS-Anfragen zu erst geforwarded werden, bevor versucht wird diese über die Root-Nameserver aufzulösen. Anstelle von `forward first` kann man auch `forward only` schreiben, dann werden alle Anfragen weitergeleitet und die Root-Nameserver werden gar nicht mehr angesprochen. Das kann für Firewall-Konfigurationen sinnvoll sein.

listen-on port 53 127.0.0.1; 192.168.0.1; ;
sagt dem BIND, auf welchen Netzwerkinterfaces und welchem Port er auf Anfragen der Clients horcht. Die Angabe `port 53` kann man sich dabei sparen, da 53 ohnehin der Standardport ist. Lässt man diesen Eintrag komplett weg, werden standardmäßig alle Interfaces verwendet.

listen-on-v6 port 53 any; ; sagt dem BIND, auf welchem Port er auf Anfragen der Clients horcht, die IPv6 verwenden. Außer `any` ist alternativ nur noch `none` erlaubt, da der Server stets auf der IPv6-Wildcard-Adresse horcht.

query-source address * port 53; Dieser Eintrag kann notwendig sein, wenn eine Firewall die externen DNS-Abfragen blockiert. So wird BIND dazu gebracht, Anfragen nach außen von Port 53 aus und nicht von den hohen Ports > 1024 zu stellen.

query-source-v6 address * port 53; Dieser Eintrag muss für Anfragen über IPv6 verwendet werden.

allow-query 127.0.0.1; 192.168.1/24; ;
bestimmt die Netze, aus denen Clients DNS-Anfragen stellen dürfen. Das `/24` ist dabei eine Kurzschreibweise für die Anzahl der Bits in der Netzmaske, in diesem Fall `255.255.255.0`.

allow-transfer ! *; ; regelt, welche Rechner Zonentransfers anfordern dürfen, dieses Beispiel unterbindet sie, aufgrund des `! *` komplett. Ohne

diesen Eintrag können Zonentransfers ohne Einschränkungen von überall angefordert werden.

statistics-interval 0; Ohne diesen Eintrag produziert BIND stündlich mehrere Zeilen Statistikmeldungen in `/var/log/messages`. Die Angabe von `0` bewirkt, dass diese komplett unterdrückt werden; hier kann man die Zeit in Minuten angeben.

cleaning-interval 720; Diese Option legt fest, in welchem Zeitabstand BIND seinen Cache aufräumt. Die Aktivität führt jedes Mal zu einem Eintrag in `/var/log/messages`. Die Zeitangabe erfolgt in Minuten. Voreingestellt sind 60 Minuten.

interface-interval 0; BIND durchsucht regelmäßig die Netzwerkschnittstellen nach neuen oder nicht mehr vorhandenen Interfaces. Setzt man diesen Wert auf `0`, so wird darauf verzichtet und BIND lauscht nur auf den beim Start gefundenen Interfaces. Alternativ kann man das Intervall in Minuten angeben. Voreingestellt sind 60 Minuten.

notify no; Das `no` bewirkt, dass keine anderen Nameserver benachrichtigt werden, wenn an den Zonendaten Änderungen vorgenommen werden oder der Nameserver neu gestartet wird.

21.7.4 Der Konfigurationsabschnitt Logging

Was und wie wohin mitprotokolliert wird, kann man beim BIND recht vielseitig konfigurieren. Normalerweise sind die Voreinstellungen ausreichend. Datei 21.12 zeigt die einfachste Form eines solchen Eintrags und unterdrückt das „Logging“ komplett.

Beispiel 21.12: *Logging wird unterdrückt*

```
logging {
        category default { null; };
};
```

21.7.5 Aufbau der Zonen-Einträge

Nach `zone` wird der Name der zu verwaltenden Domain angegeben, hier willkürlich `meine-domain.de` gefolgt von einem `in` und einem in geschweiften Klammern gesetzten Block zugehöriger Optionen; vgl. 21.13 auf der nächsten Seite.

Beispiel 21.13: *Zone-Eintrag für meine-domain.de*

```
zone "meine-domain.de" in {
       type master;
       file "meine-domain.zone";
       notify no;
};
```

Will man eine „Slave-Zone“ definieren, ändert sich nur der `type` auf `slave` und es muss ein Nameserver angegeben werden, der diese Zone als `master` verwaltet – das kann aber auch ein „slave“ sein; vgl. Datei 21.14.

Beispiel 21.14: *Zone-Eintrag für andere-domain.de*

```
zone "andere-domain.de" in {
       type slave;
       file "slave/andere-domain.zone";
       masters { 10.0.0.1; };
};
```

Die Zonen-Optionen:

type master; Das `master` legt fest, dass diese Zone auf diesem Nameserver verwaltet wird. Das setzt eine korrekt erstellte Zonendatei voraus.

type slave; Diese Zone wird von einem anderen Nameserver transferiert. Muss zusammen mit `masters` verwendet werden.

type hint; Die Zone `.` vom Typ `hint` wird für die Angabe der Root-Nameserver verwendet. Diese Zonendefinition kann man unverändert lassen.

file "meine-domain.zone" oder file "slave/andere-domain.zone"; Dieser Eintrag gibt die Datei an, in der die Zonendaten für die Domain eingetragen sind. Bei einem `slave` braucht die Datei nicht zu existieren, da ihr Inhalt von einem anderen Nameserver geholt wird. Um Master- und Slave-Dateien auseinander zu halten, gibt man für die Slave-Dateien das Verzeichnis `slave` an.

masters 10.0.0.1; ; Diesen Eintrag braucht man nur für Slave-Zonen und er gibt an, von welchem Nameserver die Zonendatei transferiert werden soll.

allow-update ! *; ; diese Option regelt den Schreibzugriff von extern auf die Zonendaten. Damit wäre es Clients möglich, sich selbst im DNS einzutragen, was aus Sicherheitsgründen nicht wünschenswert ist. Ohne diesen Eintrag, sind Zonen-Updates generell untersagt, dieses Beispiel würde daran auch nichts ändern, da `! *` ebenfalls alles verbietet.

21.7.6 Aufbau der Zonendateien

Man benötigt zwei Arten von Zonen-Dateien, die einen dienen dazu, einem Rechnernamen die IP-Adresse zuzuordnen und die anderen gehen den umgekehrten Weg und liefern zu einer gegebenen IP-Adresse den Rechnernamen.

Hinweis

Punkt (.) in Zonendateien

Eine wichtige Bedeutung hat der `.` in den Zonendateien. Werden Rechnernamen, ohne abschließenden `.` angegeben, wird immer die Zone ergänzt. Man muss also komplette Rechnernamen, die bereits mit vollständiger Domain angegeben wurden, mit einem `.` abschließen, damit die Domain nicht noch einmal dran gehängt wird. Ein fehlender Punkt oder einer an der falschen Stelle, dürfte die häufigste Fehlerursache bei der Konfiguration von Nameservern sein.

Hinweis

Den ersten Fall betrachten wir die Zonen-Datei `welt.zone`, die für die Domain `welt.all` zuständig ist; vgl. Datei 21.15.

Beispiel 21.15: *Datei /var/lib/named/welt.zone*

```
1  $TTL 2D
2  welt.all.   IN SOA      gateway  root.welt.all. (
3              2003072441  ; serial
4              1D          ; refresh
5              2H          ; retry
6              1W          ; expiry
7              2D )        ; minimum
8
9              IN NS       gateway
10             IN MX       10 sonne
```

```
11
12  gateway     IN A        192.168.0.1
13              IN A        192.168.1.1
14  sonne       IN A        192.168.0.2
15  mond        IN A        192.168.0.3
16  erde        IN A        192.168.1.2
17  mars        IN A        192.168.1.3
18  www         IN CNAME    mond
```

Zeile 1: `$TTL` definiert die Standard-TTL (engl. *Time To Live*), also zu deutsch Gültigkeitsdauer, die für alle Einträge in dieser Datei gilt: hier 2 Tage (2D = 2 days).

Zeile 2: Hier beginnt der `SOA control record` (SOA = Start of Authority):

- An erster Stelle steht hier der Name der zu verwaltenden Domain `welt.all`, diese ist mit einem `.` abgeschlossen, da ansonsten die Zone noch einmal angehängt würde. Alternativ kann man hier ein `@` schreiben, dann wird die Zone dem zugehörigen Eintrag in der `/etc/named.conf` entnommen.
- Nach dem `IN SOA` steht der Name des Nameservers, der als Master für diese Zone zuständig ist. In diesem Fall wird der Name `gateway` zu `gateway.welt.all` ergänzt, da er nicht mit einem `.` abgeschlossen ist.
- Danach folgt eine E-Mail-Adresse, der für diesen Nameserver zuständigen Person. Da das `@`-Zeichen bereits eine besondere Bedeutung hat, ist hier stattdessen einfach ein `.` zu setzen, für `root@welt.all` trägt man hier folglich `root.welt.all.` ein. Den `.` am Ende darf man hier nicht vergessen, da sonst die Zone noch angehängt würde.
- Am Ende folgt eine `(`, um die folgenden Zeilen, bis zur `)` mit in den SOA-Record einzuschließen.

Zeile 3: Die `serial number` ist eine willkürliche Zahl, die bei jeder Änderung an dieser Datei erhöht werden sollte. Sie wird benötigt, um sekundäre Nameserver (Slave-Server) über Änderungen zu informieren. Eingebürgert hat sich dafür eine zehnstellige Zahl aus Datum und fortlaufender Nummer in der Form `JJJJMMTTNN`.

Zeile 4: Die `refresh rate` gibt das Zeitintervall an, in dem Sekundär-Nameserver die `serial number` der Zone überprüfen. In diesem Fall 1 Tag (1D = 1 day).

Zeile 5: Die `retry rate` gibt den Zeitabstand an, in dem ein sekundärer Nameserver, im Fehlerfall versucht den primären Server erneut zu kontaktieren. Hier 2 Stunden (2H = 2 hours).

Zeile 6: Die `expiration time` gibt den Zeitraum an, nachdem ein sekundärer Nameserver die gecacheten Daten verwirft, wenn er keinen Kontakt zum primären Server mehr bekommen hat. Hier ist das eine Woche (1W = 1 week).

Zeile 7: Der letzte Eintrag im SOA ist die `negative caching TTL`. Er sagt aus, wie lange die Ergebnisse von DNS-Anfragen von anderen Servern gecached werden dürfen, die nicht aufgelöst werden konnten.

Zeile 9: Das `IN NS` gibt den Nameserver an, der für diese Domain zuständig ist. Auch hier gilt, dass `gateway` wieder zu `gateway.welt.all` ergänzt wird, weil es nicht mit einem `.` abgeschlossen ist. Es kann mehrere Zeilen dieser Art geben, eine für den primären und jeweils eine für jeden sekundären Nameserver. Ist für diese Zone `notify` in der `/etc/named.conf` nicht auf `no` gesetzt, werden alle hier aufgeführten Nameserver über Änderungen der Zonendaten informiert.

Zeile 10: Der MX-Record gibt den Mailserver an, der für die Domain `welt.all` die Mails annimmt und weiterverarbeitet oder weiterleitet. In diesem Beispiel ist das der Rechner `sonne.welt.all`. Die Zahl vor dem Rechnernamen ist der Präferenz-Wert, gibt es mehrere MX-Einträge, wird zuerst der Mailserver mit dem kleinsten Wert genommen und falls die Auslieferung an diesen scheitert, wird der mit dem nächst höheren Wert versucht.

Zeile 12-17: Das sind jetzt die eigentlichen Adressen-Einträge (engl. *Address Records*), in denen den Rechnernamen eine oder mehrere IP-Adressen zugeordnet werden. Die Namen stehen hier ohne abschließenden `.`, da sie ohne angehängte Domain eingetragen sind und alle um `welt.all` ergänzt werden dürfen. Dem Rechner `gateway` sind zwei IP-Adressen zugeordnet, da er über zwei Netzwerkkarten verfügt. Das `A` steht jeweils für eine traditionelle Rechner-Adresse; mit `A6` trägt man IPv6-Adressen ein und `AAAA` ist das obsolete Format für IPv6-Adressen.

Zeile 18: Mit dem Alias `www` kann auch `mond` (`CNAME` = `canonical name`) angesprochen werden.

Für die Rückwärts-Auflösung (engl. *reverse lookup*) von IP-Adressen in Rechnernamen wird die Pseudo-Domain `in-addr.arpa` zu Hilfe genommen. Diese wird dazu an den in umgekehrter Reihenfolge geschriebenen Netzanteil angehängt. Aus `192.168.1` wird dann `1.168.192.in-addr.arpa`.

Beispiel 21.16: *Umgekehrte Adress-Auflösung*

```
1
2   $TTL 2D
3   1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
4                            2003072441      ; serial
5                            1D              ; refresh
6                            2H              ; retry
7                            1W              ; expiry
8                            2D )            ; minimum
9
10                           IN NS           gateway.welt.all.
11
12  1                        IN PTR          gateway.welt.all.
13  2                        IN PTR          erde.welt.all.
14  3                        IN PTR          mars.welt.all.
```

Zeile 1: $TTL definiert die Standard-TTL, die hier für alle Einträge gilt.

Zeile 2: Der „Reverse Lookup“ soll mit dieser Datei für das Netz `192.168.1.0` ermöglicht werden. Da die Zone hier `1.168.192.in-addr.arpa` heißt, will man dies natürlich nicht an die Rechnernamen anhängen, deshalb sind diese alle komplett mit Domain und abschließendem `.` eingetragen. Der Rest entspricht dem, was im vorangegangenen Beispiel für `welt.all`, bereits beschrieben wurde.

Zeile 3-7: Siehe vorangegangenes Beispiel für `welt.all`.

Zeile 9: Diese Zeile gibt auch hier wieder den Nameserver an, der für diese Zone zuständig ist, diesmal wird aber der Name komplett mit Domain und abschließendem `.` hier eingetragen.

Zeile 11-13: Das sind die Pointer-Records, die zu einer IP-Adresse auf den zugehörigen Rechnernamen zeigen. Hier steht am Anfang der Zeile nur die letzte Stelle der IP-Adresse, ohne abschließenden `.` Wird jetzt die Zone daran angehängt und man denkt sich das `.in-addr.arpa` weg, hat man die komplette IP-Adresse in umgekehrter Reihenfolge.

Zonentransfers zwischen den verschiedenen Versionen von BIND sollten normalerweise kein Problem darstellen.

21.7.7 Sichere Transaktionen

Sichere Transaktionen kann man mithilfe der „Transaction SIGnatures“ (TSIG) verwirklichen. Dafür kommen Transaktionsschlüssel (engl. *Transaction Keys*) und -signaturen (engl. *Transaction Signatures*) zum Einsatz, deren Erzeugung und Verwendung in diesem Abschnitt beschrieben wird.

Benötigt werden sichere Transaktionen bei der Kommunikation von Server zu Server und für dynamische Aktualisierungen der Zonendaten. Eine auf Schlüsseln basierende Zugriffskontrolle bietet dafür eine weit größere Sicherheit als eine Kontrolle, die auf IP-Adressen basiert.

Ein Transaktionsschlüssel kann mit folgendem Kommando erzeugt werden (für mehr Informationen vgl. die Manualpage von `dnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Es entstehen dadurch zwei Dateien mit beispielsweise folgenden Namen:

```
Khost1-host2.+157+34265.private
Khost1-host2.+157+34265.key
```

Der Schlüssel ist in beiden Dateien enthalten (z.B. `ejIkuCyyGJwwuN3xAteKgg==`). Zur weiteren Verwendung sollte `Khost1-host2.+157+34265.key` auf sicherem Wege (zum Beispiel mit `scp`) auf den entfernten Rechner übertragen und dort in der `/etc/named.conf` eingetragen werden, um eine sichere Kommunikation zwischen `host1` und `host2` zu bewirken:

```
key host1-host2. {
  algorithm hmac-md5;
  secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

Achtung

Zugriffsrechte von /etc/named.conf

Achten Sie darauf, dass die Zugriffsrechte auf `/etc/named.conf` eingeschränkt bleiben; die Vorgabe ist `0640` für `root` und die Gruppe `named`; alternativ kann man die Schlüssel auch in ein eigene geschützte Datei auslagern und diese dann includieren.

Achtung

Damit auf dem Server `host1` der Schlüssel für `host2` mit der Beispielsadresse `192.168.2.3` verwendet wird, muss auf dem Server in der `/etc/named.conf` eingetragen werden:

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

In den Konfigurationsdateien von `host2` müssen entsprechende Einträge vorgenommen werden.

Zusätzlich zu den ACLs auf Basis von IP-Adressen und Adress-Bereichen, soll man, um sichere Transaktionen auszuführen, TSIG-Schlüssel hinzufügen; ein Beispiel dafür kann so aussehen:

```
allow-update { key host1-host2. ;};
```

Mehr dazu findet man im *BIND Administrator Reference Manual* zu `update-policy`.

21.7.8 Zonendaten dynamisch aktualisieren

Dynamische Aktualisierungen (engl. *Dynamic Update*) ist der Terminus, der das Hinzufügen, Ändern oder Löschen von Einträgen in den Zonen-Dateien eines Masters bezeichnet. Beschrieben ist dieser Mechanismus im RFC 2136.

Dynamische Aktualisierungen werden je Zone mit den Optionen `allow-update` oder `update-policy` bei den Zonen-Einträgen konfiguriert. Zonen, die dynamisch aktualisiert werden, sollten nicht von Hand bearbeitet werden.

Mit `nsupdate` werden die zu aktualisierenden Einträge an den Server übertragen; zur genauen Syntax vgl. die Manualpage von `nsupdate`. Die Aktualisierung sollte aus Sicherheitsüberlegungen heraus unbedingt über sichere Transaktionen (TSIG) geschehen; vgl. Abschnitt 21.7.7 auf der vorherigen Seite.

21.7.9 DNSSEC

DNSSEC (engl. *DNS Security*) ist im RFC 2535 beschrieben; welche Tools für den Einsatz von DNSSEC zur Verfügung stehen, ist im BIND-Manual beschrieben.

Eine sichere Zone muss einen oder mehrere Zonen-Schlüssel haben; diese werden, wie die Host-Schlüssel, auch mit `dnssec-keygen` erzeugt. Zur Verschlüsselung wählt man momentan DSA.

Die öffentlichen Schlüssel (engl. *public keys*) sollten in die Zonen-Dateien mit `$INCLUDE` eingebunden werden.

Alle Schlüssel werden mit `dnssec-makekeyset` zu einem Set zusammengefasst, das auf sicherem Wege an die übergeordnete Zone (engl. *Parent Zone*) zu übertragen ist, um dort mit `dnssec-signkey` signiert zu werden. Die bei der Signierung erzeugten Dateien müssen zum Signieren von Zonen mit `dnssec-signzone` verwendet werden und die dabei entstandenen Dateien sind schließlich in `/etc/named.conf` für die jeweilige Zone einzubinden.

21.7.10 Konfiguration mit YaST

Das YaST DNS-Modul dient der Konfiguration eines eigenen DNS-Servers im lokalen Netz. Dieses Modul kennt zwei verschiedene Funktionsmodi:

Wizard Konfiguration Beim ersten Start des Moduls werden von Ihnen als Administrator einige grundlegende Entscheidungen verlangt. Nach Abschluss der initialen Konfiguration ist der Server grob vorkonfiguriert und prinzipiell einsatzbereit.

Experten-Konfiguration Der Expertenmodus dient fortgeschritteneren Konfigurationsaufgaben wie ACL, Logging, TSIG-Keys u. a.

Wizard-Konfiguration

Der Wizard gliedert sich in drei Dialoge auf, von denen Sie an geeigneter Stelle in die Expertenkonfiguration abzweigen können.

Installation des DNS-Servers: Forwarder-Einstellungen
Diesen Dialog (siehe Abbildung 21.9 auf der nächsten Seite erhalten Sie beim ersten Start dieses Moduls. Entscheiden Sie sich, ob Sie die eine Liste von Forwarders vom PPP Daemon bei der Einwahl per DSL oder ISDN erhalten möchten ('PPP Daemon legt Forwarders fest') oder sie selber eingeben ('Forwarders manuell festlegen').

Installation des DNS-Servers: DNS-Zonen
Die Einträge in diesem Modul, werden in der Experteninstallation (siehe 21.7.10 auf Seite 517) erklärt.

Installation des DNS-Servers: Wizard beenden
Im Abschluss können Sie das Startverhalten des DNS-Servers (an oder aus) und die LDAP-Unterstützung aktivieren (siehe Abbildung 21.10 auf Seite 516).

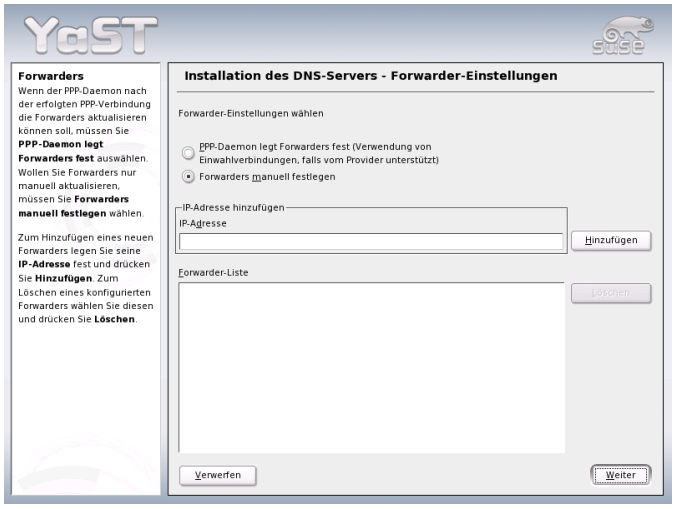

Abbildung 21.9: *Installation des DNS-Servers: Forwarders*

Expertenkonfiguration

Beim ersten Start des Moduls öffnet YaST ein Fenster mit mehreren Konfigurationsmöglichkeiten. Nach dessen Beendigung ist der DNS-Server prinzipiell einsatzbereit:

DNS-Server: Start Unter der Überschrift 'Systemstart' können Sie den DNS-Server ein ('An') oder ausschalten ('Aus'). Über den Button 'DNS-Server nun starten' können Sie den DNS-Server starten.

Mittels 'LDAP-Unterstützung aktiv' stellen Sie die LDAP-Unterstützung ein, wodurch es möglich ist die Zonendateien mit der LDAP-Datenbank abzugleichen. Werden die Zoneninformationen in der LDAP-Datenbank geändert, werden beim nächsten Restart oder Reload des DNS-Servers diese aktualisiert.

DNS-Server: Forwarders Dieser Dialog ist derselbe, den Sie auch beim Start im Wizard-Konfiguration erhalten (siehe 21.7.10 auf der vorherigen Seite).

DNS-Server: Grundlegende Einstellungen
Unter dieser Rubrik legen Sie grundsätzliche Optionen fest. Aus dem Menü 'Option' wählen Sie den entsprechenden Eintrag aus und geben im Eingabefeld 'Wert' den Wert ein. Mittels 'Hinzufügen' fügen Sie die Option zu der Liste hinzu.

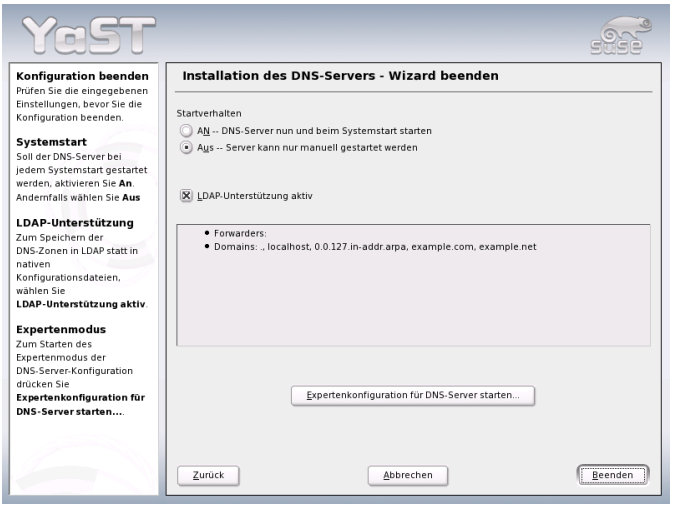

Abbildung 21.10: *Installation des DNS-Servers: Wizard beenden*

DNS-Server: Protokollieren Innerhalb dieser Rubrik stellen Sie das Verhalten des DNS-Servers ein, was und wohin er seine Protokolldatei schreiben soll.

Unter 'Protokolltyp' spezifizieren Sie, wohin der DNS-Servers seine Meldungen hineinschreibt. Sie können es dem System überlassen ('In Systemprotokoll protokollieren' nach `/var/log/messages`), oder Sie legen die Datei explizit fest ('In Datei protokollieren'). Haben Sie letzeres gewählt, können Sie noch die maximale Dateigröße in Megabyte und die Anzahl dieser Logfiles angeben.

Unter 'Zusätzliches Protokollieren' können Sie weitere Optionen einstellen: 'Anfragen protokollieren' protokolliert *jede* Anfrage. Die Logdatei kann daher sehr voluminös werden. Sie sollten diese Option nur für Debugging-Zwecke aktivieren. Um zwischen DHCP-Server und DNS-Server ein Zonenupdate durchzuführen, wählen Sie 'Zonen-Updates protokollieren'. Um den Datenverkehr beim Transfer der Zonendaten (Zonentransfer) vom Master zum Slave zu protokollieren, aktivieren Sie die Option 'Zonen-Transfers protokollieren' (siehe Abbildung 21.11 auf der nächsten Seite).

DNS-Server: ACLs ACLs (engl. *Access Control Lists*) sind Zugriffsbeschränkungen, die Sie in diesem Fenster festlegen können.

Geben Sie unter 'Name' eine sprechende Bezeichnung ein und unter

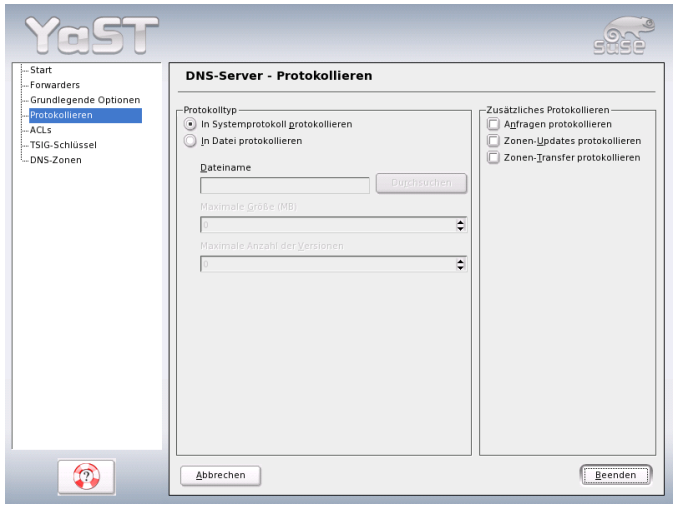

Abbildung 21.11: *DNS-Server: Protokollieren*

'Wert' eine IP-Adresse (mit oder ohne Netzmaske) bei dem Sie den Zugriff erlauben möchten. Zum Beispiel:

```
{ 10.10/16; }
```

Die Syntax der Konfigurationsdatei verlangt geschweifte Klammern und ein abschließendes Semikolon.

DNS-Server: TSIG-Schlüssel TSIG (engl. *Transaction SIGnature*) wird im Abschnitt 21.7.7 auf Seite 512 beschrieben. In erster Linie sind TSIG für die Kommunikation zwischen DHCP und DNS relevant.

Um einen Transaktionsschlüssel zu erstellen, geben Sie unter 'Schlüssel-ID' einen sprechenden Namen ein und die Datei in der der Schlüssel gespeichert werden soll (Eingabefeld 'Dateiname'). Bestätigen Sie mit 'Hinzufügen'.

Falls Sie schon einen Schlüssel besitzen, lassen Sie das Eingabefeld 'Schlüssel-ID' leer und wählen unter 'Dateiname' die entsprechende Datei aus. Bestätigen Sie ebenfalls mit 'Hinzufügen'.

DNS-Server: DNS-Zonen Diese Rubrik ist in mehrere Dialogfenster unterteilt und ist dafür zuständig Zonen-Dateien zu verwalten (siehe Abschnitt 21.7.6 auf Seite 508).

Unter ‘Name der Zone’ tragen Sie den neuen Namen einer Zone ein. Um reverse Zonen zu erzeugen muss der Zonenname auf `.in-addr.arpa` enden. Wählen Sie den Typ (Master oder Slave) mit ‘Zonentyp’ aus (siehe Abbildung 21.12). Durch ‘Zone bearbeiten...’ können Sie weitere Einstellungen festlegen.

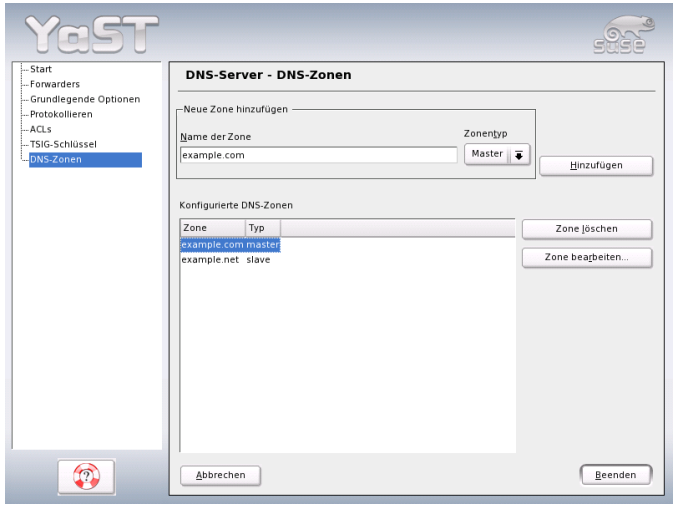

Abbildung 21.12: *DNS-Server: DNS-Zonen*

DNS-Server: Slave Zonen-Editor Diese Dialogbox erhalten Sie, wenn Sie unter dem Punkt 21.7.10 auf der vorherigen Seite als Zonentyp ‘Slave’ angewählt haben. Geben Sie unter ‘Master DNS-Server’ den Masterserver an, der vom Slave abgefragt werden soll. Falls Sie den Zugriff beschränken möchten, können Sie vorher definierte ACLs in der Liste auswählen (siehe Abbildung 21.13 auf der nächsten Seite).

DNS-Server: Master Zonen-Editor
Diese Dialogbox erhalten Sie, wenn Sie unter dem Punkt 21.7.10 auf der vorherigen Seite als Zonentyp ‘Master’ angewählt haben. Sie unterteilt sich in mehrere Ansichten: Grundlagen (die momentane Seite, die Sie sehen), NS-Einträge, MX-Einträge, SOA und Einträge. Alle folgenden beschriebenen Punkte beziehen sich auf die genannten.

In Abbildung 21.14 auf Seite 520 legen Sie Dynamische DNS-Einstellungen und die Zugriffsbedingungen für Zonentransfers an

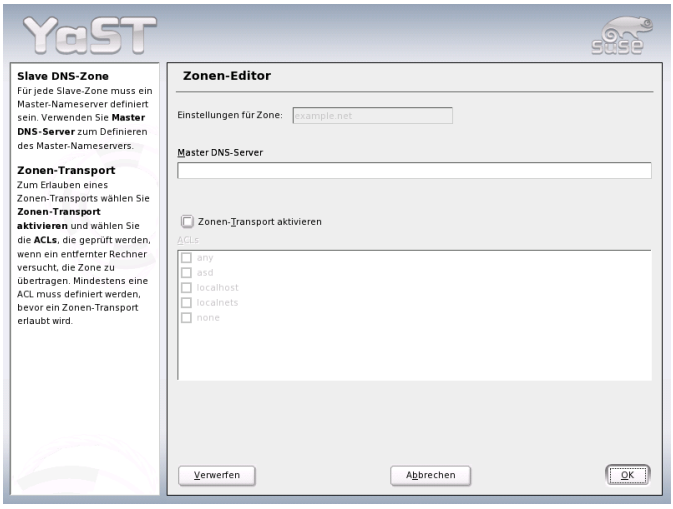

Abbildung 21.13: *DNS-Server: Slave Zonen-Editor*

Clients und Slave Nameserver fest. Um dynamische Updates der Zonen zu erlauben, wählen Sie 'Dynamische Updates erlauben' und den entsprechenden Transaktions-Schlüssel (TSIG) aus. Achten Sie darauf, dass vorher schon ein Schlüssel definiert wurde, bevor Sie den Updatevorgang starten.

Um Zonentransfers zu erlauben, müssen Sie die entsprechenden ACLs wählen. Sie müssen ACLs vorher bereits definiert haben.

DNS-Server: Zonen-Editor (NS-Einträge)
Dieser Dialog legt alternative Nameserver für diese Zonen fest. Achten Sie darauf, dass der eigene Nameserver in der Liste enthalten ist. Um einen neuen Eintrag vorzunehmen, geben Sie unter 'Hinzuzufügender Nameserver' den entsprechenden Namen ein und bestätigen Sie mit 'Hinzufügen' (siehe Abbildung 21.15 auf Seite 521).

DNS-Server: Zonen-Editor (MX-Einträge)
Um einen neuen Mailserver für die aktuelle Zone zur bestehenden Liste einzufügen, geben Sie die zugehörige Adresse und die Priorität ein. Bestätigen Sie mit 'Hinzufügen' (siehe Abbildung 21.16 auf Seite 522).

DNS-Server: Zonen-Editor (SOA) Die Anzeige zur *SOA Record Configuration* (siehe Abbildung 21.17 auf Seite 523) wird verwendet, um

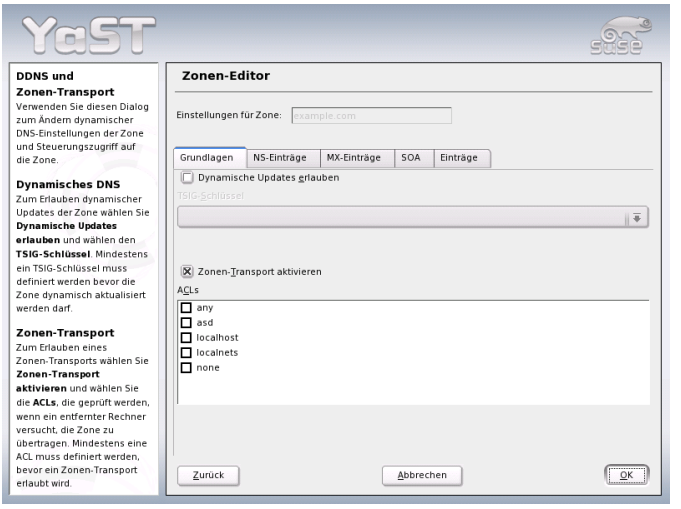

Abbildung 21.14: *DNS-Server: Zonen-Editor (Grundlagen)*

SOA-Einträge (*Start of Authority*) anzulegen. Die Bedeutung der einzelnen Optionen kann im Beispiel 21.15 auf Seite 508 nachgelesen werden. Achten Sie darauf, dass diese Option nicht bei dynamischen Zonen in Kombination mit LDAP zur Verfügung steht.

DNS-Server: Zonen-Editor (Einträge)
Dieser Dialog verwaltet eine Liste von Zuordnungen von Namen zu IP-Adressen. Geben Sie im Eingabefeld unter 'Eintragsschlüssel' den Hostnamen ein und wählen Sie den Typ aus (gleichnamiges Dropdown-Menü). 'A-Record' ist der Haupteintrag; 'CNAME' ist ein Alias und unter 'MX-Relay' wird der Eintrag (Name) durch den Wert (Value) überschrieben.

21.7.11 Weitere Informationen

Hinzuweisen ist insbesondere auf das *BIND Administrator Reference Manual*, das online in `/usr/share/doc/packages/bind9/` zu finden ist, sowie auf die dort genannten RFCs und die mit BIND 9 mitgelieferten Manual-Pages.

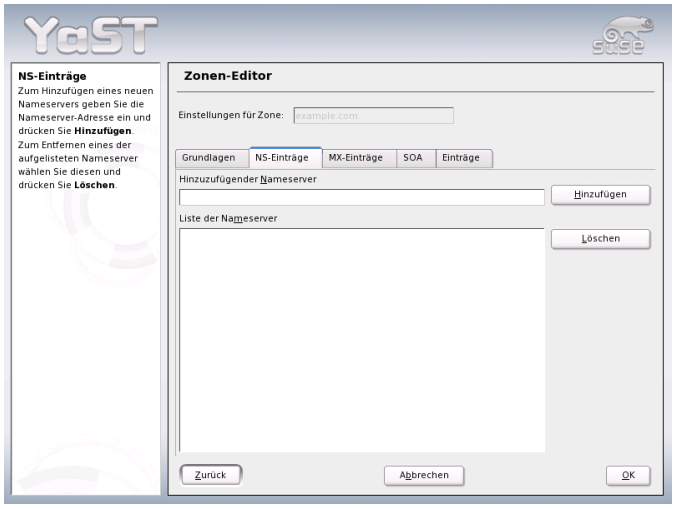

Abbildung 21.15: *DNS-Server: Zonen-Editor (NS-Einträge)*

21.8 LDAP – Ein Verzeichnisdienst

Innerhalb einer vernetzten Arbeitsumgebung ist es entscheidend, wichtige Informationen strukturiert und schnell abrufbar bereitzuhalten. Dieses Problem löst ein Verzeichnisdienst, der ähnlich den Gelben Seiten (engl. *Yellow Pages*) im normalen Alltagsleben die gesuchten Informationen in gut strukturierter, schnell durchsuch- und abrufbarer Form bereithält.

Im Idealfall existiert ein zentraler Server, der die Daten in einem Verzeichnis vorhält und über ein bestimmtes Protokoll an alle Clients im Netzwerk verteilt. Die Daten sollten derart strukturiert sein, dass ein möglichst breites Spektrum von Anwendungen darauf zugreifen kann. So muss nicht jedes Kalendertool oder jeder E-Mailclient seine eigenen Datenbanken vorhalten, sondern kann auf den zentralen Bestand zurückgreifen. Dies verringert den Verwaltungsaufwand für die betreffenden Informationen beträchtlich. Die Verwendung eines offenen und standardisierten Protokolls wie LDAP (engl. *Lightweight Directory Access Protocol*) stellt sicher, dass möglichst viele Clientapplikationen auf solche Informationen zugreifen können.

Ein Verzeichnis in diesem Kontext ist eine Art von Datenbank, die daraufhin optimiert ist, besonders gut und schnell les- und durchsuchbar zu sein:

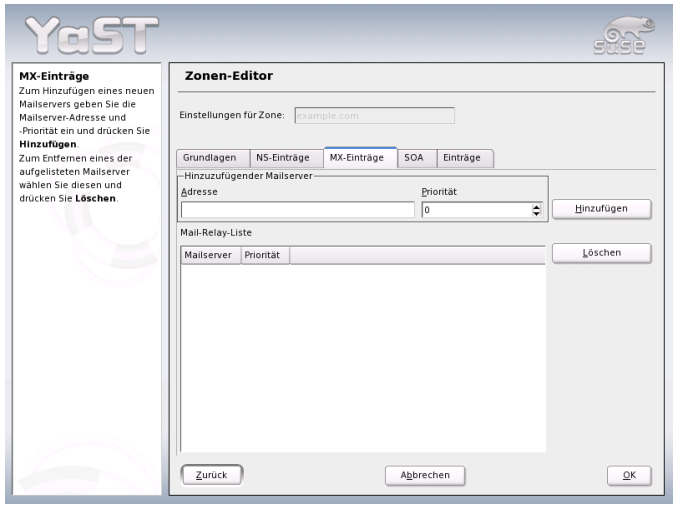

Abbildung 21.16: *DNS-Server: Zonen-Editor (MX-Einträge)*

- Um zahlreiche (gleichzeitige) Lesezugriffe zu ermöglichen, wird der Schreibzugriff auf einige wenige Aktualisierungen seitens des Administrators begrenzt. Herkömmliche Datenbanken sind daraufhin optimiert, in kurzer Zeit ein möglichst großes Datenvolumen aufzunehmen.

- Da Schreibzugriffe nur sehr eingeschränkt ausgeführt werden sollen, verwaltet man über einen Verzeichnisdienst möglichst unveränderliche, *statische* Informationen. Die Daten innerhalb einer konventionellen Datenbank ändern sich typischerweise sehr häufig (*dynamische* Daten). Telefonnummern in einem Mitarbeiterverzeichnis ändern sich nicht annähernd so häufig wie zum Beispiel die Zahlen, die in der Buchhaltung verarbeitet werden.

- Werden statische Daten verwaltet, sind Updates der bestehenden Datensätze sehr selten. Bei der Arbeit mit dynamischen Daten, besonders wenn es um Datensätze wie Bankkonten und Buchhaltung geht, steht die Konsistenz der Daten im Vordergrund. Soll eine Summe an einer Stelle abgebucht werden, um sie an anderer Stelle hinzuzufügen, müssen beide Operationen gleichzeitig – innerhalb einer „Transaktion“ ausgeführt werden, um die Ausgeglichenheit des gesamten Datenbestandes sicherzustellen. Datenbanken unterstützen solche

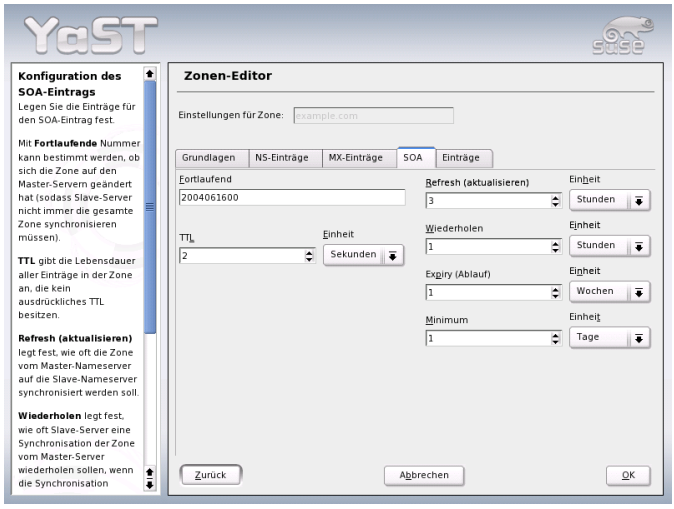

Abbildung 21.17: *DNS-Server: Zonen-Editor (SOA)*

Transaktionen, Verzeichnisse nicht. Kurzfristige Inkonsistenzen der Daten sind bei Verzeichnissen durchaus akzeptabel.

Das Design eines Verzeichnisdienstes wie LDAP ist nicht dazu ausgelegt, komplexe Update- oder Abfragemechanismen zu unterstützen. Alle auf diesen Dienst zugreifende Anwendungen sollen möglichst leicht und schnell Zugriff haben.

Verzeichnisdienste gab und gibt es, nicht nur in der Unix-Welt, viele. Novells NDS, Microsofts ADS, Banyans Street Talk und den OSI-Standard X.500.

LDAP war ursprünglich als eine schlanke Variante des DAP (engl. *Directory Access Protocol*) geplant, das für den Zugriff auf X.500 entwickelt wurde. Der X.500-Standard regelt die hierarchische Organisation von Verzeichniseinträgen.

LDAP ist um einige Funktionen des DAP erleichtert und kann plattformübergreifend und vor allem ressourcenschonend eingesetzt werden, ohne dass man auf die in X.500 definierten Eintragshierarchien verzichten müsste. Durch die Verwendung von TCP/IP ist es wesentlich einfacher, Schnittstellen zwischen aufsetzender Applikation und LDAP-Dienst zu realisieren.

Mittlerweile hat sich LDAP weiterentwickelt und kommt immer häufiger als Stand-alone-Lösung ohne X.500-Unterstützung zum Einsatz. Mit LDAPv3 (der Protokollversion, die Sie mit dem installierten Paket `openldap2` vorliegen haben) unterstützt LDAP so genannte *Referrals*, mit deren Hilfe sich verteilte Datenbanken realisieren lassen. Ebenfalls neu ist die Nutzung von SASL (engl. *Simple Authentication and Security Layer*) als Authentifizerungs- und Sicherungsschicht.

LDAP kann nicht nur zur Datenabfrage von X.500-Servern eingesetzt werden, wie ursprünglich geplant war. Es gibt mit slapd einen Open Source Server, mit dem Objektinformationen in einer lokalen Datenbank gespeichert werden können. Ergänzt wird er durch slurpd, der für die Replikation mehrerer LDAP-Server zuständig ist.

Das Paket `openldap2` besteht im Wesentlichen aus zwei Programmen.

slapd Ein Stand-alone-LDAPv3-Server, der Objektinformationen in einer BerkeleyDB-basierten Datenbank verwaltet.

slurpd Dieses Programm ermöglicht es, Änderungen an den Daten des lokalen LDAP-Servers an andere im Netz installierte LDAP-Server zu replizieren.

Zusätzliche Tools zur Systempflege
slapcat, slapadd, slapindex

21.8.1 LDAP versus NIS

Traditionell verwendet der Unix-Systemadministrator zur Namensauflösung und Datenverteilung im Netzwerk den NIS-Dienst. Auf einem zentralen Server werden die Konfigurationsdaten aus den `/etc`-Dateien und Verzeichnissen `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` und `services` über die Clients im Netz verteilt. Als bloße Textdateien sind diese Dateien ohne größeren Aufwand wartbar. Allerdings wird die Verwaltung größerer Datenmengen aufgrund mangelnder Strukturierung schwierig. NIS ist nur für Unix-Plattformen ausgelegt, was einen Einsatz als zentrale Datenverwaltung im heterogenen Netz unmöglich macht.

Das Einsatzgebiet des LDAP-Dienstes ist im Gegensatz zu NIS nicht auf reine Unix-Netze beschränkt. Windows Server (ab 2000) unterstützen LDAP als Verzeichnisdienst. Ebenso bietet auch Novell einen LDAP-Dienst an. Zudem ist er nicht auf die oben genannten Aufgabengebiete beschränkt.

Das LDAP-Prinzip kann für beliebige Datenstrukturen verwendet werden, die zentral verwaltet werden sollen. Einige Anwendungsbeispiele wären zum Beispiel:

- Einsatz anstelle eines NIS-Servers
- Mailrouting (postfix, sendmail)
- Adressbücher für Mailclients wie Mozilla, Evolution, Outlook, ...
- Verwaltung von Zonenbeschreibungen für einen BIND9-Nameserver

Diese Aufzählung kann beliebig fortgesetzt werden, da LDAP im Gegensatz zu NIS erweiterbar ist. Die klar definierte hierarchische Struktur der Daten hilft bei der Verwaltung sehr großer Datenmengen, da sie besser durchsuchbar ist.

21.8.2 Aufbau eines LDAP-Verzeichnisbaums

Ein LDAP-Verzeichnis hat eine baumartige Struktur. Alle Einträge (Objekte genannt) im Verzeichnis haben eine definierte Position innerhalb dieser Hierarchie. Diese Hierarchie wird als *Directory Information Tree* oder kurz DIT bezeichnet. Der komplette Pfad zum gewünschten Eintrag, der ihn eindeutig identifiziert, wird *Distinguished Name* oder DN genannt. Die einzelnen Knoten auf dem Weg zu diesem Eintrag werden *Relative Distinguished Name* oder RDN genannt. Objekte können generell zwei verschiedenen Typen zugeordnet werden:

Container Diese Objekte können wieder andere Objekte enthalten. Solche Objektklassen sind `Root` (Wurzelelement des Verzeichnisbaums, das nicht real existiert), `c` (engl. *country*), `ou` (engl. *OrganizationalUnit*), und `dc` (engl. *domainComponent*). Vergleichbar ist dieses Modell auch mit Verzeichnissen (Ordnern) im Dateisystem.

Blatt Diese Objekte sitzen am Ende eines Astes. Ihnen sind keine anderen Objekte untergeordnet. Beispiele sind `Person`, `InetOrgPerson` oder `groupofNames`.

An der Spitze der Verzeichnishierarchie liegt ein Wurzelelement `Root`. Diesem können in der nächsten Ebene entweder `c` (engl. *country*), `dc` (engl. *domainComponent*) oder `o` (engl. *organization*) untergeordnet werden.

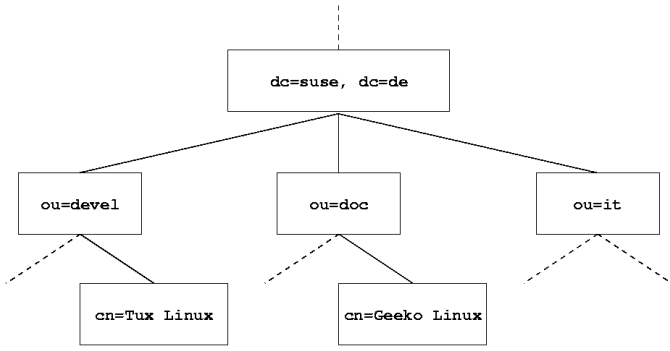

Abbildung 21.18: *Aufbau eines LDAP-Verzeichnisses*

Die Beziehungen innerhalb eines LDAP-Verzeichnisbaums werden am folgenden Beispiel (siehe Abbildung 21.18) deutlich.

Die gesamte Abbildung umfasst einen fiktiven *Directory Information Tree*. Abgebildet sind die Einträge (engl. *entries*) auf drei Ebenen. Jeder Eintrag entspricht in der Abbildung einem Kästchen. Der vollständige gültige *Distinguished Name* für den fiktiven SuSE-Mitarbeiter `Geeko Linux` ist in diesem Fall `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Er setzt sich zusammen, indem der RDN `cn=Geeko Linux` zum DN des Vorgängereintrags `ou=doc,dc=suse,dc=de` hinzugefügt wird.

Die globale Festlegung, welche Typen von Objekten im DIT gespeichert werden sollen, geschieht über ein *Schema*. Der Typ eines Objekts wird durch die *Objektklasse* festgelegt. Die Objektklasse bestimmt, welche Attribute dem betreffenden Objekt zugeordnet werden müssen bzw. können. Ein Schema muss demnach Definitionen aller Objektklassen und Attribute enthalten, die im gewünschten Einsatzszenario verwendet werden. Es existieren einige allgemein gebräuchliche Schemata (siehe RFC 2252 und 2256). Allerdings können auch benutzerdefinierte Schemata geschaffen werden oder mehrere Schemata ergänzend zueinander verwendet werden, wenn es die Umgebung erfordert, in der der LDAP-Server betrieben werden soll.

Tabelle 21.9 auf der nächsten Seite gibt einen kleinen Überblick über die im Beispiel verwendeten Objektklassen aus `core.schema` und `inetorgperson.schema` samt zwingend erforderlicher Attribute und den passender Attributwerte.

Tabelle 21.9: *Häufig verwendete Objektklassen und Attribute*

Objektklasse	Bedeutung	Beispieleintrag	erforderl. Attribute
dcObject	*domainComponent* (Namensbestandteile der Domain)	suse	dc
organizationalUnit	*organizationalUnit* (Organisationseinheit)	doc	ou
inetOrgPerson	*inetOrgPerson* (Personenbezogene Daten für Intra-/Internet)	Geeko Linux	sn und cn

In Beispiel 21.17 sehen Sie einen Auszug aus einer Schema-Anweisung mit Erklärungen, der Ihnen beim Verstehen der Syntax neuer Schemata hilft.

Beispiel 21.17: *Auszug aus schema.core (Zeilennummerierung aus Verständnisgründen)*

```
...
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2     DESC 'RFC2256: organizational unit this object belongs to'
#3     SUP name )
...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5   DESC 'RFC2256: an organizational unit'
#6      SUP top STRUCTURAL
#7   MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory $
      x121Address $ registeredAddress $ destinationIndicator $
      preferredDeliveryMethod $ telexNumber $
      teletexTerminalIdentifier $ telephoneNumber $
      internationaliSDNNumber $ facsimileTelephoneNumber $ street $
      postOfficeBox $ postalCode $ postalAddress $
      physicalDeliveryOfficeName $ st $ l $ description) )
...
```

Als Beispiel dient der Attributtyp `organizationalUnitName` und die zugehörige Objektklasse `organizationalUnit`. In Zeile 1 wird der Name des Attributs, sein eindeutiger OID (*Object Identifier*) (numerisch) sowie das Kürzel des Attributs gelistet. In Zeile 2 wird mit `DESC` eine kurze

Beschreibung des Attributs eingeleitet. Hier ist auch der zugehörige RFC genannt, auf den die Definition zurückgeht. `SUP` in Zeile 3 weist auf einen übergeordneten Attributtyp hin, zu dem dieses Attribut gehört.

Die Definition der Objektklasse `organizationalUnit` beginnt in Zeile 4 wie bei der Attributsdefinition mit einem OID und dem Namen der Objektklasse. In Zeile 5 lesen Sie eine Kurzbeschreibung der Objektklasse. Zeile 6 mit dem Eintrag `SUP top` besagt, dass diese Objektklasse keine Unterklasse einer anderen Objektklasse ist. Zeile 7, beginnend mit `MUST`, führt alle Attributtypen auf, die zwingend in einem Objekt vom Typ `organizationalUnit` verwendet werden *müssen*. In Zeile 8 sind nach `MAY` alle Attributtypen gelistet, die in Zusammenhang mit dieser Objektklasse verwendet werden *können*.

Eine sehr gute Einführung in den Umgang mit Schemata finden Sie in der Dokumentation zu OpenLDAP in Ihrem installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

21.8.3 Serverkonfiguration mit slapd.conf

Wenn das System installiert ist, ist `/etc/openldap/slapd.conf` als vollständige Konfigurationsdatei für den LDAP-Server vorhanden. Im Folgenden werden die einzelnen Einträge kurz beleuchtet und notwendige Anpassungen erklärt. Einträge mit führendem # sind inaktiv. Um solche Einträge zu aktivieren, entfernen Sie dieses Kommentarzeichen.

Globale Anweisungen in slapd.conf

Beispiel 21.18: *slapd.conf: Include-Anweisung für Schemata*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Mit dieser ersten Anweisung in `slapd.conf` wird das Schema spezifiziert, nach dem Ihr LDAP-Verzeichnis organisiert ist (siehe Beispiel 21.18). Der Eintrag `core.schema` ist zwingend erforderlich. Sollten Sie weitere Schemata benötigen, fügen Sie sie hinter dieser Anweisung ein (als Beispiel wurde hier `inetorgperson.schema` hinzugefügt). Weitere verfügbare Schemata finden Sie im Verzeichnis `/etc/openldap/schema/`. Soll NIS durch einen analogen LDAP-Dienst ersetzt werden, binden Sie hier die Schemata `cosine.schema` und `rfc2307bis.schema` ein. Informationen zu dieser Problematik entnehmen Sie der mitgelieferten OpenLDAP-Dokumentation.

Beispiel 21.19: *slapd.conf: pidfile und argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Diese zwei Dateien enthalten die PID (engl. *process id*) und einige Argumente, mit denen der slapd Prozess gestartet wird. An dieser Stelle ist keine Änderung erforderlich.

Beispiel 21.20: *slapd.conf: Zugangskontrolle*

```
# Sample Access Control
#       Allow read access of root DSE
#        Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
              by users read
              by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

Beispiel 21.20 ist der Ausschnitt aus `slapd.conf`, der die Zugangskontrolle zum LDAP-Verzeichnis auf dem Server regelt. Die Einstellungen, die hier im globalen Abschnitt der `slapd.conf` gemacht werden, gelten, soweit nicht im datenbankspezifischen Abschnitt eigene Zugangsregeln aufgestellt werden, die sie überschreiben. So wie hier wiedergegeben, können alle Benutzer lesend auf das Verzeichnis zugreifen, aber nur der Administrator (`rootdn`) kann auf diesem Verzeichnis schreiben. Das Regeln der Zugriffsrechte unter LDAP ist ein sehr komplexer Prozess. Daher hier einige Grundregeln, die Ihnen helfen, diesen Vorgang nachzuvollziehen.

- Jede Zugangsregel ist folgendermaßen aufgebaut:

  ```
  access to <what> by <who> <access>
  ```

- ⟨*what*⟩ steht für das Objekt oder Attribut, zu dem Sie Zugang gewähren. Sie können einzelne Verzeichnisäste explizit durch separate Regeln schützen oder aber mit Hilfe regulärer Ausdrücke ganze Regionen des Verzeichnisbaums mit einer Regel abarbeiten. slapd wird alle Regeln in der Reihenfolge evaluieren, in der diese in der Konfigurationsdatei eingeführt wurden. Demnach führen Sie allgemeinere Regeln immer hinter spezifischeren auf. Die erste Regel, die slapd als zutreffend bewertet, wird ausgewertet und alle folgenden Einträge ignoriert.

- ⟨*who*⟩ legt fest, wer Zugriff auf die unter ⟨*what*⟩ festgelegten Bereiche erhalten soll. Auch hier können Sie durch die Verwendung passender regulärer Ausdrücke viel Aufwand sparen. Wiederum wird slapd nach dem ersten „Treffer“ mit der Auswertung von ⟨*who*⟩ abbrechen, d.h. spezifischere Regeln sollten wieder vor den allgemeineren aufgeführt werden. Folgende Einträge sind möglich (siehe Tabelle 21.10):

Tabelle 21.10: *Zugangsberechtigte Benutzergruppen*

Bezeichner	**Bedeutung**
*	ausnahmslos alle Benutzer
`anonymous`	nicht authentifizierte („anonyme“) Benutzer
`users`	authentifizierte Benutzer
`self`	Benutzer, die mit dem Zielobjekt verbunden sind
`dn.regex=<regex>`	Alle Benutzer, auf die dieser reguläre Ausdruck zutrifft

- ⟨*access*⟩ spezifiziert die Art des Zugriffs. Es wird hier unterschieden zwischen den in Tabelle 21.11 aufgeführten Möglichkeiten:

Tabelle 21.11: *Zugriffsarten*

Bezeichner	**Bedeutung**
`none`	Zutritt verboten
`auth`	zur Kontaktaufnahme mit dem Server
`compare`	zum vergleichenden Zugriff auf Objekte

`search`	zur Anwendung von Suchfiltern
`read`	Leserecht
`write`	Schreibrecht

slapd vergleicht die vom Client angeforderte Berechtigung mit der in `slapd.conf` gewährten. Werden dort höhere oder gleiche Rechte gewährt als der Client anfordert, wird dem Client der Zugang erlaubt. Fordert der Client höhere Rechte als dort angegeben, erhält er keinen Zugang.

Beispiel 21.21 zeigt ein einfaches Beispiel für eine Zugangskontrolle, die Sie durch Einsatz regulärer Ausdrücke beliebig ausgestalten können.

Beispiel 21.21: *slapd.conf: Beispiel für Zugangskontrolle*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
   by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
   by user read
   by * none
```

Diese Regel besagt, dass zu allen `ou`-Einträgen nur der jeweilige Administrator schreibenden Zugang hat. Die übrigen authentifizierten Benutzer sind leseberechtigt und der Rest der Welt erhält keinen Zugang.

Hinweis

Aufstellen von Access Regeln

Falls es keine `access to` Regel oder keine `by <who>` Anweisung greift, ist der Zugriff verboten. Nur explizit angegebene Zugriffsrechte werden gewährt. Für den Fall, dass keine einzige Regel aufgestellt wird, gilt das Standardprinzip: Schreibrecht für den Administrator und Leserecht für die übrige Welt.

Hinweis

Detailinformationen und eine Beispielkonfiguration für LDAP-Zugriffsrechte finden Sie in der Online-Dokumentation des installierten `openldap2`-Pakets. Neben der Möglichkeit, Zugriffskontrollen über die zentrale Serverkonfigurationsdatei (`slapd.conf`) zu verwalten, gibt es den Weg über ACIs (engl. *Access Control Information*). Mittels ACIs können die Zugangsinformationen zu einzelnen Objekten im LDAP-Baum

selbst abgespeichert werden. Da diese Art der Zugangskontrolle noch nicht sehr verbreitet ist und von den Entwicklern als experimentell eingestuft wird, verweisen wir an dieser Stelle auf die entsprechende Dokumentation auf den Seiten des OpenLDAP-Projekts: `http://www.openldap.org/faq/data/cache/758.html`.

Datenbankspezifische Anweisungen in slapd.conf

Beispiel 21.22: *slapd.conf: Datenbankspezifische Anweisungen*

```
database ldbm
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

In der ersten Zeile dieses Abschnitts (siehe Beispiel 21.22) wird der Datenbanktyp festgelegt, hier LDBM. Über `suffix` in der zweiten Zeile wird festgelegt, für welchen Teil des LDAP-Verzeichnisbaumes dieser Server verantwortlich sein soll. Das folgende `rootdn` legt fest, wer Administratorzugriff auf diesen Server besitzt. Der hier angegebene Benutzer muss keinen LDAP-Eintrag besitzen oder als „normaler“ Benutzer existieren. Mit der `rootpw` Anweisung wird das Administratorpasswort gesetzt. Sie können hier statt `secret` auch den mit slappasswd erzeugten Hash des Administratorpassworts eintragen. Die `directory` Anweisung gibt das Verzeichnis an, in dem die Datenbankverzeichnisse auf dem Server abgelegt sind. Die letzte Anweisung, `index objectClass eq`, bewirkt, dass ein Index über die Objektklassen gepflegt wird. Ergänzen Sie hier unter Umständen einige Attribute, nach denen Ihrer Erfahrung nach am häufigsten gesucht wird. Wenn nachgestellt für die Datenbank eigene `Access` Regeln definiert werden, werden diese statt der globalen `Access` Regeln angewendet.

Start und Stopp des Servers

Ist der LDAP-Server fertig konfiguriert und sind alle gewünschten Einträge im LDAP-Verzeichnis nach dem unten beschriebenen Muster (siehe Abschnitt 21.8.4) erfolgt, starten Sie den LDAP-Server als Benutzer `root` durch Eingabe des folgenden Befehls:

```
rcldap start
```

Möchten Sie den Server manuell wieder stoppen, geben Sie entsprechend `rcldap stop` ein. Die Statusabfrage über den Laufzustand des LDAP-Servers nehmen Sie mit `rcldap status` vor. Um Start und Stopp des Servers beim Starten bzw. Herunterfahren des betreffenden Rechners zu automatisieren, nutzen Sie den YaST Runlevel-Editor (vergleiche Abschnitt 11.5 auf Seite 297) oder Sie legen die entsprechenden Links der Start- und Stoppskripten mittels `insserv` auf der Kommandozeile selbst an (siehe Abschnitt 11.4.1 auf Seite 296).

21.8.4 Handhabung von Daten im LDAP-Verzeichnis

OpenLDAP gibt Ihnen als Administrator eine Reihe von Programmen an die Hand, mit denen Sie die Daten im LDAP-Verzeichnis verwalten können. Im Folgenden werden die vier wichtigsten von ihnen zum Hinzufügen, Löschen, Durchsuchen und Verändern des Datenbestandes kurz behandelt.

Daten in ein LDAP-Verzeichnis eintragen

Vorausgesetzt, die Konfiguration Ihres LDAP-Servers in `/etc/openldap/slapd.conf` ist korrekt und einsatzfähig, d.h. sie enthält die passenden Angaben für `suffix`, `directory`, `rootdn`, `rootpw` und `index`, können Sie nun mit der Aufnahme von Einträgen beginnen. OpenLDAP bietet hierfür den Befehl `ldapadd`. Aus praktischen Gründen sollten Sie Objekte nach Möglichkeit gebündelt zur Datenbank hinzufügen. Zu diesem Zweck kennt LDAP das so genannte LDIF-Format (engl. *LDAP Data Interchange Format*). Eine LDIF-Datei ist eine einfache Textdatei, die aus beliebig vielen Attribut-Wert-Paaren bestehen kann. Für die zur Verfügung stehenden Objektklassen und Attribute schauen Sie in den in `slapd.conf` angegebenen Schemadateien nach. Die LDIF-Datei zum Anlegen eines groben Gerüsts für das Beispiel aus Abbildung 21.18 auf Seite 526 sähe folgendermaßen aus (siehe Beispiel 21.23 auf der nächsten Seite):

Beispiel 21.23: *Beispiel für eine LDIF-Datei*

```
# Die Organisation SUSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# Die Organisationseinheit Entwicklung (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# Die Organisationseinheit Dokumentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# Die Organisationseinheit Interne EDV (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

Hinweis

Kodierung der LDIF-Dateien

LDAP arbeitet mit UTF-8 (Unicode). Umlaute müssen demnach bei der Eingabe korrekt kodiert werden. UTF-8 ist seit SUSE LINUX 9.1 als Standard eingestellt und wird von allen gängigen Editoren unterstützt. Sollten Sie Ihre Umgebung auf ein anderes Encoding umgestellt haben (vgl. Abschnitt 10.7 auf Seite 286), müssen Sie entweder auf die Eingabe von Umlauten überhaupt verzichten oder iconv zum Umkodieren der Eingaben nach UTF-8 verwenden.

Hinweis

Speichern Sie die Datei unter `<datei>.ldif` ab und übergeben Sie sie mit folgendem Befehl an den Server:

```
ldapadd -x -D <dn des Administrators> -W -f <datei>.ldif
```

Die erste Option `-x` gibt an, dass in diesem Fall auf Authentifizierung über SASL verzichtet wird. `-D` kennzeichnet den Benutzer, der diese Operation vornimmt; hier geben Sie den gültigen DN des Administrators an, wie sie in `slapd.conf` konfiguriert wurde. Im konkreten Beispiel wäre dies `cn=admin,dc=suse,dc=de`. Mit `-W` umgehen Sie die Eingabe des Passworts auf der Kommandozeile (Klartext) und aktivieren eine separate Passwortabfrage. Das betreffende Passwort wurde vorher in `slapd.conf` unter `rootpw` eingerichtet. `-f` übergibt die Datei. In Beispiel 21.24 sehen Sie Aufruf von `ldapadd` im Detail.

Beispiel 21.24: *ldapadd von beispiel.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f beispiel.ldif
Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Die Benutzerdaten der einzelnen Mitarbeiter können Sie in separaten LDIF-Dateien angeben. Mit dem folgenden Beispiel `tux.ldif` (siehe Beispiel 21.25) wird der Mitarbeiter `Tux` dem neuen LDAP-Verzeichnis hinzugefügt:

Beispiel 21.25: *LDIF-Datei für Tux*

```
# Der Mitarbeiter Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Eine LDIF-Datei kann beliebig viele Objekte enthalten. Sie können ganze Verzeichnisbäume am Stück an den Server übergeben oder auch nur Teile davon wie zum Beispiel einzelne Objekte. Wenn Sie Ihre Daten relativ häufig ändern müssen, empfiehlt sich eine feine Stückelung in einzelne Objekte, da Ihnen dann das mühsame Suchen nach dem zu ändernden Objekt in einer großen Datei erspart bleibt.

Daten im LDAP-Verzeichnis ändern

Stehen in Ihrem Datensatz Änderungen an, verwenden Sie das Tool `ldapmodify`. Am einfachsten ändern Sie zuerst die betreffende LDIF-Datei und übergeben anschließend die geänderte Datei wieder an den LDAP-Server. Um zum Beispiel die Telefonnummer des Mitarbeiters `Tux` von `+49 1234 567-8` auf `+49 1234 567-10` zu ändern, editieren Sie die LDIF-Datei wie in Beispiel 21.26 gezeigt.

Beispiel 21.26: *Geänderte LDIF Datei tux.ldif*

```
# Der Mitarbeiter Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Die geänderte Datei importieren Sie mit dem folgenden Befehl in das LDAP-Verzeichnis:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Alternativ können Sie `ldapmodify` auch direkt die zu ändernden Attribute auf der Kommandozeile angeben. Hierbei gehen Sie wie folgt vor:

1. Rufen Sie `ldapmodify` auf und geben Sie Ihr Passwort ein:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W
   Enter LDAP password:
   ```

2. Geben Sie Ihre Änderungen nach der folgenden Syntax in genau dieser Reihenfolge an:

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Detaillierte Informationen zu `ldapmodify` und zur Syntax lesen Sie in der Manualpage von `ldapmodify` nach.

Daten aus einem LDAP-Verzeichnis suchen oder auslesen

OpenLDAP bietet mit ldapsearch ein Kommandozeilenwerkzeug zum Durchsuchen und Auslesen von Daten im LDAP-Verzeichnis. Ein einfaches Suchkommando hätte folgende Syntax:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

Die Option `-b` legt die Suchbasis, d.h. den Baumbereich, in dem gesucht werden soll, fest. In diesem Fall ist dies `dc=suse,dc=de`. Möchten Sie eine verfeinerte Suche auf bestimmten Unterbereichen des LDAP-Verzeichnisses ausführen (z.B. nur über die Abteilung `devel`), geben Sie diesen Bereich mittels `-b` an. `ldapsearch -x` legt die Verwendung einfacher Authentifizierung fest. Mit `(objectClass=*)` legen Sie fest, dass Sie alle in Ihrem Verzeichnis enthaltenen Objekte auslesen wollen. Verwenden Sie dieses Kommando nach dem Aufbau eines neuen Verzeichnisbaumes, um zu überprüfen, ob alle Ihre Einträge korrekt übernommen wurden und der Server in der gewünschten Form antwortet. Weitere Informationen zum Gebrauch von `ldapsearch` finden Sie in entsprechenden Manualpage (`man ldapsearch`).

Daten aus einem LDAP-Verzeichnis löschen

Löschen Sie nicht mehr erwünschte Einträge mittels `ldapdelete`. Die Syntax ähnelt der der oben beschriebenen Kommandos. Um beispielsweise den Eintrag von `Tux Linux` im Ganzen zu löschen, geben Sie folgendes Kommando ein:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

21.8.5 LDAP-Server: Konfiguration mit YaST

YaST unterstützt die Einrichtung eines LDAP Servers. Dieser Server kann neben der Benutzerauthentifizierung weitere Dienste im Netz übernehmen (wie z. B. die Verwaltung der Mail-, DNS- und DHCP-Konfigurationen). Die Verwendung von LDAP für diese Zwecke legen Sie während der Installation fest. Der folgende Abschnitt beschreibt die LDAP-Serverkonfiguration mit YaST, wie sie über das separate YaST-Modul 'Netzwerkdienste' → 'LDAP-Server' vorgenommen wird.

Im ersten Dialog entscheiden Sie darüber, ob der LDAP-Server konfiguriert und beim Systembootgestartet werden soll. Über den Button ‘Konfigurieren...’ gelangen Sie in den ersten Dialog zur eigentlichen Konfiguration des Servers (siehe Abbildung 21.19).

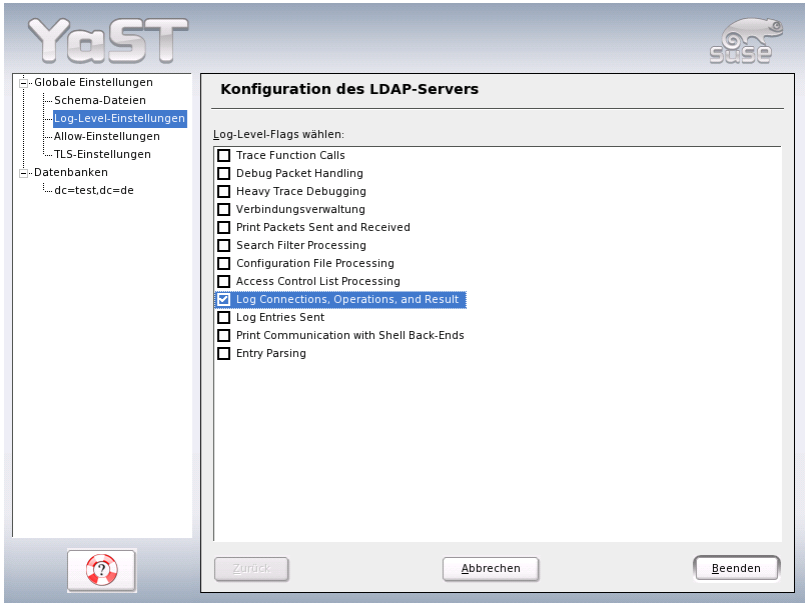

Abbildung 21.19: *YaST OpenLDAP Server-Konfiguration: Log-Level*

Im linken Teil des Dialogfensters sehen Sie in einer Baumansicht alle per YaST konfigurierbaren Eigenschaften des LDAP-Servers angezeigt. Dies sind zum einen die ‘Globale Einstellungen’ (‘Log-Level-Einstellungen’, ‘Allow-Einstellungen’ und ‘TLS-Einstellungen’) und zum anderen die ‘Datenbanken’. Im rechten Bereich des Dialogfensters erscheint jeweils der Konfigurationsdialog zum in der Baumansicht selektierten Unterpunkt.

Über die ‘Log-Level-Einstellungen’ legen Sie den „Geschwätzigkeitsgrad“ des LDAP-Servers fest. Wählen Sie aus einer festdefinierten Liste die gewünschten Logging-Optionen. Je mehr Optionen Sie aktivieren, desto umfangreicher werden die Protokoll-Dateien.

Mit den ‘Allow-Einstellungen’ regeln Sie, welche Arten von Verbindungsaufnahme der LDAP-Server erlauben soll (siehe Abb. 21.20 auf der nächsten Seite).

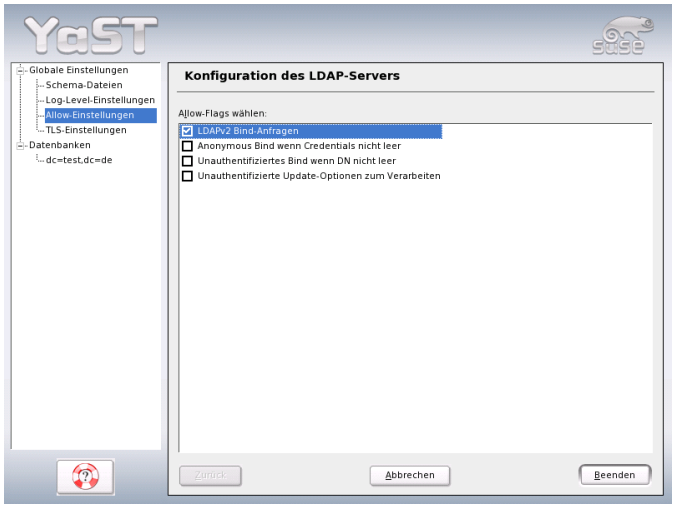

Abbildung 21.20: *YaST OpenLDAP Server-Konfiguration: Allow*

Die einzelnen 'Allow-Flags' haben die folgende Bedeutung:

bind_v2 Diese Option erlaubt die Annahme von Verbindungsanfragen (engl. *bind requests*) auch von Clients der Vorversion (LDAPv2).

bind_anon_cred Normalerweise lehnt der LDAP-Server alle Authentifizierungsversuche ab, bei denen entweder DN oder Passwort (Credentials) leer bleiben. Mit `bind_anon_cred` ist es erlaubt, ein Passwort aber keinen DN anzugeben. In diesem Fall wird eine anonyme Verbindung aufgebaut.

bind_anon_dn Diese Option gewährt unauthentifizierte (anonyme) Verbindungen, wenn ein DN aber kein Passwort übergeben wird.

update_anon Diese Option erlaubt unauthentifizierte (anonyme) Updateoperationen. Diese Art des Zugangs unterliegt den Zugangbeschränkungen durch ACLs etc. (siehe Abschnitt 21.8.3 auf Seite 528).

Nach der Konfiguration der 'Allow-Flags' fahren Sie mit der Konfiguration der 'TLS-Einstellungen' fort. Hier legen Sie fest, wie die Kommunikation zwischen Server und Clients abgesichert werden soll (siehe Abb. 21.21 auf der nächsten Seite).

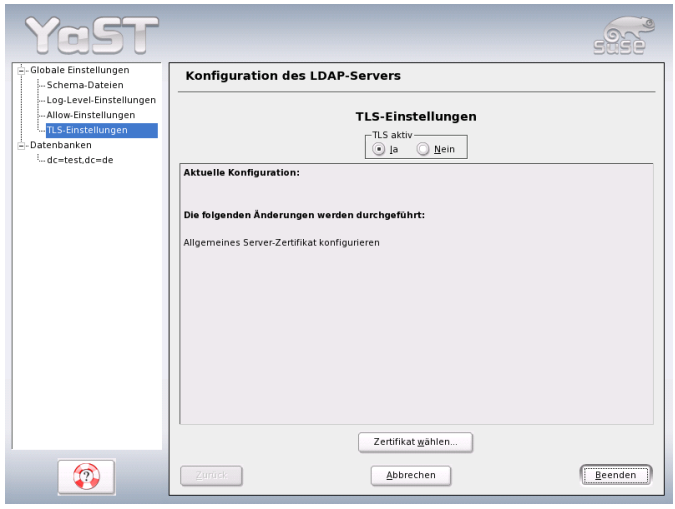

Abbildung 21.21: *YaST OpenLDAP Server-Konfiguration: TLS*

Legen Sie zunächst per Radiobutton fest, ob die TLS/SSL-Verschlüsselung der Kommunikation zwischen Server uns Clients aktiviert werden soll. Anschließend wählen Sie das zu verwendende Zertifikat über den Button 'Zertifikat wählen...' aus. Ein Popup erscheint (siehe Abb. 21.22), in dem Sie den Typ des verwendeten Zertifikats festlegen. Sie können wählen, ob Sie mit 'Allgemeines Server-Zertifikat verwenden' das bei der Installation des SUSE LINUX Enterprise Server automatisch per YaST angelegte Zertifikat verwenden wollen oder ein externes Zertifikat importieren wollen ('Zertifikat importieren'). Wurde bei der Installation kein allgemeines Server-Zertifikat angelegt, öffnet sich sofort der Import-Dialog.

Abbildung 21.22: *YaST OpenLDAP Server-Konfiguration: Zertifikat wählen*

Entscheiden Sie sich für das Importieren eines externen Zertifikats, fragt

YaST die Dateinamen und -Pfade für das Zertifikat, dessen Schlüsseldatei und das CA-Zertifikat ab (siehe Abb. 21.23). Geben Sie diese Daten ein und verlassen Sie den Dialog mit ‘Ok’.

Abbildung 21.23: *YaST OpenLDAP Server Konfiguration: Zertifikat importieren*

Sind die globalen Einstellungen des LDAP-Servers abgeschlossen, konfigurieren Sie die auf dem Server existierenden Datenbanken. Klicken Sie in der Baumansicht auf ‘Datenbanken’, erhalten Sie im rechten Teil der Dialogansicht (siehe Abb. 21.24) eine Liste der verfügbaren Datenbanken. Klicken Sie ‘Datenbank hinzufügen...’, um eine neue Datenbank hinzuzufügen.

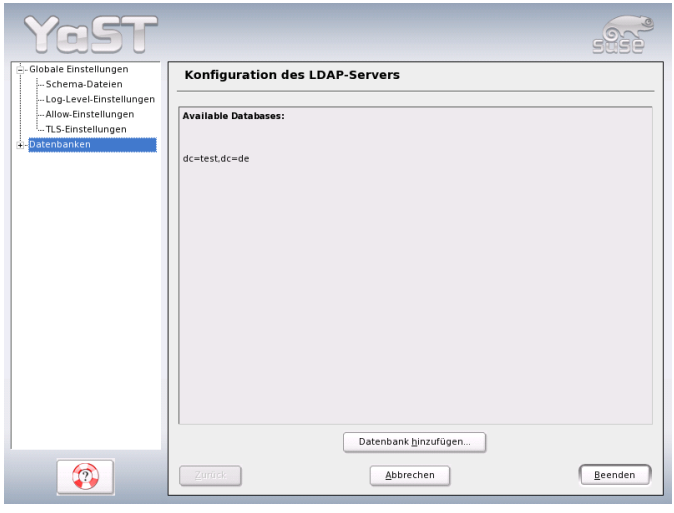

Abbildung 21.24: *YaST OpenLDAP Server Konfiguration: Datenbankübersicht*

YaST fragt nun die erforderlichen Einträge mittels einer Eingabemaske ab (siehe Abb. 21.25 auf der nächsten Seite). Im Feld ‘Base DN’ tragen Sie die

Basis-DN Ihres LDAP-Servers ein. In das Feld ‘Root DN’ tragen Sie den DN des Administrators ein, der den Server verwalten soll. Aktivieren Sie hier die Checkbox ‘Base DN anhängen’, müssen Sie lediglich den `cn` des Administrators eingeben, den Rest vervollständigt das System automatisch. Geben Sie nun in den entsprechenden Feldern das Root-Passwort des Server-Administrators ein und wählen Sie den Verschlüsselungsalgorithmus für das Passwort (‘crypt’, ‘smd5’, ‘ssha’, ‘sha’). Weiterhin gibt es die Option ‘plain’ für Plaintext-Passworte, die aber aus Sicherheitsgründen nicht verwendet werden sollte. Bestätigen Sie Ihre Einstellungen mit ‘OK’, gelangen Sie zurück in den Ausgangsdialog.

Abbildung 21.25: *YaST OpenLDAP Server Konfiguration: Neue Datenbank*

Möchten Sie eine bereits angelegte Datenbank mit YaST ändern, selektieren Sie in der Baumansicht im linken Dialogteil deren Basis-DN. Im rechten Dialogteil erscheint nun eine ähnliche Eingabemaske wie beim Neuanlegen einer Datenbank. Lediglich die Basis-DN ist ausgegraut und kann nicht geändert werden (siehe Abb. 21.26 auf der nächsten Seite).

Sobald Sie diesen Dialog mit ‘Beenden’ verlassen, ist Ihr LDAP-Server in den Grundzügen konfiguriert und einsatzbereit. Für tiefergehende Konfiguration editieren Sie die Serverkonfiguration unter `/etc/openldap/slapd.conf` manuell und starten den Server dann erneut.

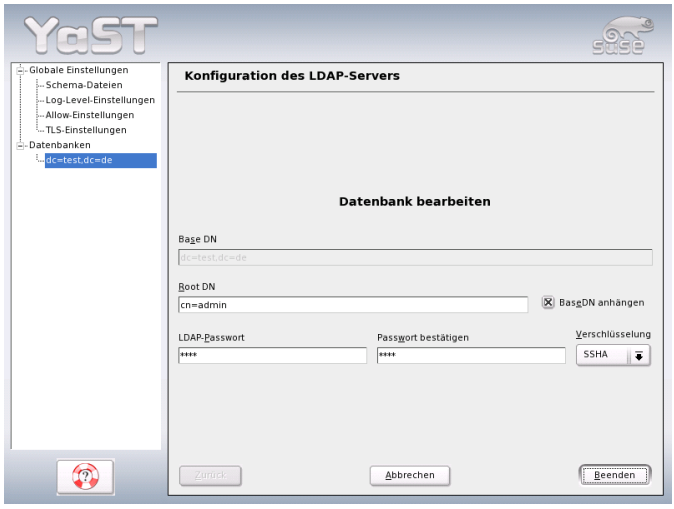

Abbildung 21.26: *YaST OpenLDAP Server Konfiguration: Datenbank ändern*

21.8.6 Der YaST LDAP-Client

YaST unterstützt LDAP-gestützte Benutzerverwaltung. Um diese Unterstützung zu aktivieren, wenn dies nicht schon während der Installation erfolgt ist, rufen Sie das Modul 'Netzwerkdienste' → 'LDAP-Client' auf. YaST installiert und konfiguriert die unten beschriebenen LDAP-Anpassungen für PAM und NSS automatisch.

Genereller Ablauf

Um die Funktion des YaST LDAP-Client-Moduls zu verstehen, sollten Sie über die Abläufe im Hintergrund auf Ihrem Clientrechner grob Bescheid wissen. Zunächst werden, sobald Sie bei der Installation die Verwendung von LDAP zur Netzwerkauthentifizierung aktivieren oder das YaST-Modul aufrufen, die Pakete `pam_ldap` und `nss_ldap` installiert und die beiden entsprechenden Konfigurationsdateien angepasst. Mit `pam_ldap` wird das PAM-Modul benutzt, das für die Vermittlung zwischen Loginprozessen und LDAP-Verzeichnis als Quelle der Authentifizierungsdaten zuständig ist. Das zuständige Softwaremodul `pam_ldap.so` wird installiert und die PAM-Konfiguration angepasst (siehe Beispiel 21.27 auf der nächsten Seite).

Beispiel 21.27: *pam_unix2.conf angepasst für LDAP*

```
auth:       use_ldap nullok
account:    use_ldap
password:   use_ldap nullok
session:    none
```

Wollen Sie zusätzliche Dienste manuell für den Gebrauch von LDAP konfigurieren, muss das PAM-LDAP-Modul in die dem Dienst entsprechende PAM-Konfigurationsdatei unter `/etc/pam.d/` eingefügt werden. Bereits für einzelne Dienste angepasste Konfigurationsdateien finden Sie unter `/usr/share/doc/packages/pam_ldap/pam.d/`. Kopieren Sie die entsprechenden Dateien nach `/etc/pam.d/`.

Über `nss_ldap` passen Sie die Namensauflösung der `glibc` über den `nsswitch`-Mechanismus an die Verwendung von LDAP an. Mit Installation dieses Paketes wird unter `/etc/` eine neue, angepasste Datei `nsswitch.conf` abgelegt. Mehr zur Funktion von `nsswitch.conf` finden Sie unter Abschnitt 21.3.1 auf Seite 473. Für die Benutzerverwaltung bzw. -authentifizierung mittels LDAP müssen in Ihrer `nsswitch.conf` folgende Zeilen vorhanden sein (vgl. Beispiel 21.28:

Beispiel 21.28: *Anpassungen in nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Diese Zeilen weisen die Resolver-Bibliothek der `glibc` an, als Quelle für die Authentifizierungsdaten und Benutzerdaten zuerst die lokal auf dem System die entsprechenden Dateien unter `/etc/` auszuwerten und zusätzlich auf den LDAP-Server zuzugreifen. Testen Sie diesen Mechanismus, indem Sie mittels des Kommandos `getent passwd` beispielsweise den Inhalt der Benutzerdatenbank auslesen. Sie sollten im Resultat sowohl lokale Benutzer auf Ihrem System als auch alle auf dem LDAP-Server hinterlegten Benutzer in einer Übersicht erhalten.

Soll verhindert werden, dass sich normale, per LDAP verwaltete Benutzer auf dem Server mit ssh oder login einloggen können, müssen `/etc/passwd` und `/etc/group` um eine Zeile ergänzt werden. `/etc/passwd` um `+::::::/sbin/nologin` und `/etc/group` um `+:::` .

Konfiguration des LDAP-Clients

Nachdem `nss_ldap` und `pam_ldap` sowie `/etc/passwd` und `/etc/group` von YaST korrekt angepasst wurden, können Sie nun in der ersten YaST-Maske mit den eigentlichen Konfigurationsarbeiten beginnen.

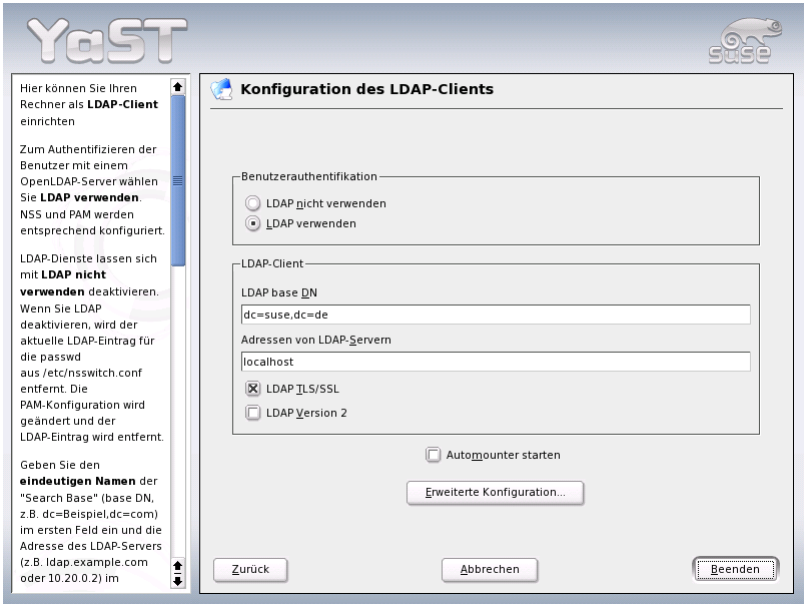

Abbildung 21.27: *YaST: Konfiguration des LDAP-Clients*

Im ersten Dialog (siehe Abbildung 21.27) aktivieren Sie per Radiobutton die Verwendung von LDAP zur Benutzerauthentifizierung und tragen unter ‘LDAP Base DN’ die Suchbasis auf dem Server ein, unterhalb der alle Daten auf dem LDAP-Server liegen. Im zweiten Eingabefeld ‘Adresse des LDAP-Servers’ tragen Sie die Adresse ein, unter der der LDAP-Server zu erreichen ist. Unterstützt Ihr Server TLS/SSL, aktivieren Sie die Checkbox ‘LDAP TLS/SSL’, um verschlüsselte Kommunikation zwischen Client und Server zu ermöglichen. Wollen Sie entfernte Verzeichnisse in Ihr Dateisystem einhängen, aktivieren Sie die Checkbox ‘Automounter starten’. Möchten Sie als Administrator Daten aktiv auf dem Server verändern, klicken Sie auf ‘Erweiterte Konfiguration’.

Der folgende Dialog ist zweigeteilt: Im oberen Bereich nehmen Sie allgemeine Einstellungen zu Benutzern und Gruppen vor, die das Verhalten des

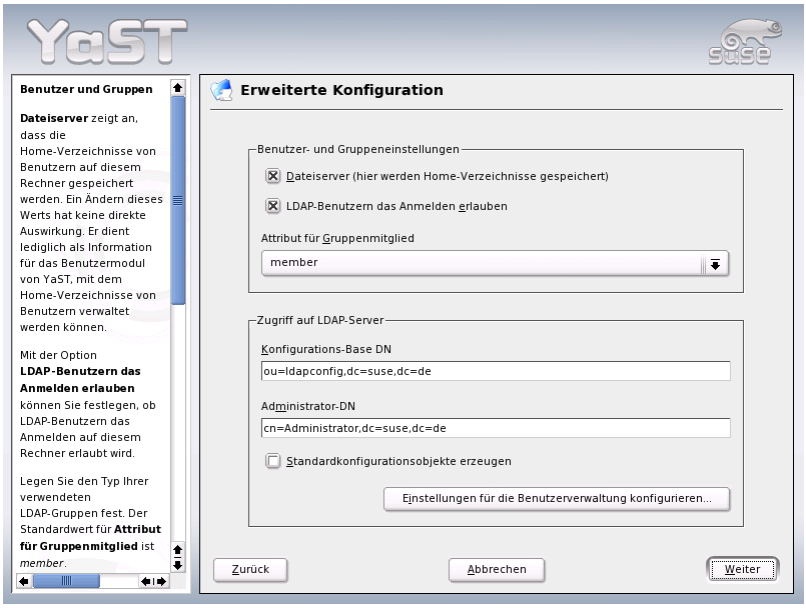

Abbildung 21.28: *YaST: Erweiterte Konfiguration*

YaST Benutzer-Moduls bestimmen. Im unteren Bereich tragen Sie die Zugangsdaten zum LDAP-Server ein. Die Einstellungen zu Benutzern und Gruppen beschränken sich auf die folgenden Einträge:

Dateiserver Ist dieses System ein Dateiserver und verwaltet `/home` Verzeichnisse der Benutzer? Das Aktivieren der Checkbox gibt dem YaST Benutzer-Modul Hinweise, wie mit den Benutzerverzeichnissen auf diesem System umzugehen ist.

LDAP-Benutzern das Anmelden erlauben
Aktivieren Sie diese Checkbox, um den über LDAP verwalteten Benutzern ein Einloggen auf dem System zu ermöglichen.

Attribut für Gruppenmitglied Bestimmen Sie den zu verwendenden Typ von LDAP-Gruppen. Zur Auswahl stehen: ‘member’ (Standardeinstellung) und ‘uniquemember’.

Hinweis

Einsatz des YaST-Clients

Der YaST LDAP-Client wird eingesetzt, um die YaST-Module zur Benutzer- und Gruppenverwaltung anzupassen und bei Bedarf zu erweitern. Ausserdem haben Sie die Möglichkeit, Schablonen mit Standardwerten für die einzelnen Attribute zu definieren, um eigentliche Erfassung der Daten zu vereinfachen. Die hier erstellten Vorgaben werden selbst als LDAP-Objekte im LDAP-Verzeichnis abgelegt. Die Erfassung der Benutzerdaten erfolgt weiterhin über die normalen YaST-Modulmasken. Die erfassten Informationen werden als Objekte im LDAP-Verzeichnis abgelegt.

Hinweis

Um Konfigurationen auf dem LDAP-Server zu ändern, tragen Sie in diesem Dialog die benötigten Zugangsdaten ein (siehe Abbildung 21.28 auf der vorherigen Seite). Dies sind 'Konfigurations-Base DN', unterhalb der alle Konfigurationsobjekte abgelegt sind, und 'Administrator-DN'. Um Einträge auf dem LDAP-Server zu bearbeiten, klicken Sie auf 'Einstellungen für die Benutzerverwaltung konfigurieren'. Es erscheint ein Popupfenster, in dem Sie Ihr LDAP-Passwort eingeben, um sich am Server zu authentifizieren. Anhand der ACLs oder ACIs auf dem Server wird Ihnen Zugang zu den Konfigurationsmodulen auf dem Server gewährt.

Im Dialog zur Modulkonfiguration haben Sie die Möglichkeit, bestehende Konfigurationsmodule auszuwählen und abzuändern, neue Module anzulegen oder Vorlagen (engl. *Templates*) für solche Module zu erstellen und zu bearbeiten (siehe Abbildung 21.29 auf der nächsten Seite). Zum Ändern eines Wertes innerhalb eines Konfigurationsmoduls oder zum Umbenennen eines Moduls wählen Sie über die Combobox oberhalb der Inhaltsansicht des aktuellen Moduls den Modultyp aus. In der Inhaltsansicht erscheint nun eine tabellarische Auflistung aller in diesem Modul erlaubten Attribute und zugeordneten Werte. Hier finden sich neben allen gesetzten Attributen auch alle anderen Attribute, die per benutztem Schema erlaubt sind, aber derzeit nicht verwendet werden. Möchten Sie ein Modul kopieren, ändern Sie lediglich `cn`. Um einzelne Attributwerte zu ändern, selektieren Sie diese in der Inhaltsübersicht und klicken auf 'Bearbeiten'. Ein Dialogfenster öffnet sich, in dem Sie die alle zum Attribut gehörigen Einstellungen ändern können. Übernehmen Sie Ihre Änderungen mit 'OK'.

Möchten Sie die bereits bestehenden Module um ein neues Modul ergänzen, klicken Sie auf den 'Neu' Button oberhalb der Inhaltsüber-

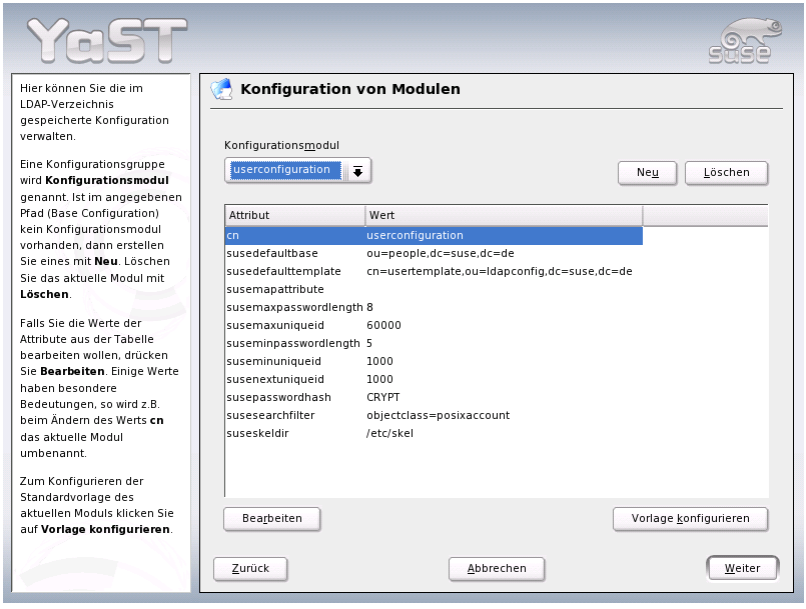

Abbildung 21.29: *YaST: Modulkonfiguration*

sicht. Nachfolgend geben Sie im sich öffnenden Dialog die Objektklasse des neuen Moduls (hier entweder `suseuserconfiguration` oder `susegroupconfiguration`) und den Namen des neuen Moduls ein. Verlassen Sie diesen Dialog mit ‘OK’, wird das neue Modul in die Auswahlliste der vorhandenen Module aufgenommen und kann über die Combobox an- und abgewählt werden. Wollen Sie das aktuell selektierte Modul löschen, klicken Sie auf den ‘Löschen’ Button.

Die YaST-Module zur Gruppen- und Benutzerverwaltung binden Vorlagen mit sinnvollen Standardwerten ein, wenn Sie diese zuvor mittels des YaST LDAP-Clients definiert haben. Um ein Template entsprechend Ihren Vorstellungen zu editieren, klicken Sie auf den Button ‘Vorlage konfigurieren’. Entweder werden bereits vorhandene, änderbare Templates oder ein leerer Eintrag, der ebenfalls in die Maske zur Templatebearbeitung führt, im Drop-Down-Menü angezeigt. Wählen Sie eines und konfigurieren Sie in der folgenden Maske ‘Konfiguration der Objektvorlage’ die Eigenschaften dieses Templates. Diese Maske gliedert sich in zwei tabellarische Übersichtsfenster. Im oberen Fenster sind alle allgemeinen Templateattribute aufgelistet. Legen Sie deren Werte fest, wie es zu Ihrem Einsatzszenario passt oder lassen Sie manche leer. „Leere“ Attribute werden auf dem

Abbildung 21.30: *YaST: Attributsänderung in der Modulkonfiguration*

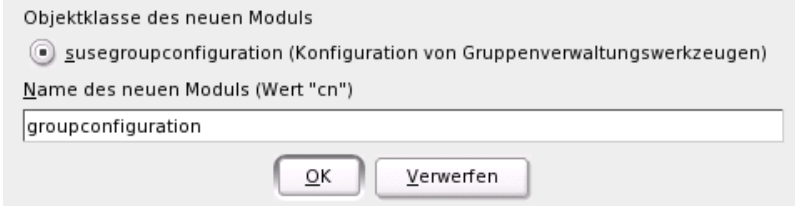

Abbildung 21.31: *YaST: Neues Modul erstellen*

LDAP-Server gelöscht.

Die zweite Übersicht (‘Standardwerte für neue Objekte’) listet alle Attribute des zugehörigen LDAP-Objekts (hier: Gruppen- oder Benutzerkonfiguration), für die Sie einen Standardwert definieren. Sie können weitere Attribute und deren Standardwerte hinzufügen, bestehende Attribut-Wertpaare editieren und ganze Attribute löschen. Ebenso wie ein Modul lässt sich ein Template durch Änderung des `cn` Eintrags einfach kopieren, um ein neues Template anzulegen. Verbinden Sie das Template mit dem zugehörigen Modul, indem Sie den Attributwert von `susedefaulttemplate` des Moduls wie bereits oben beschrieben auf den DN des angepassten Templates setzen.

Hinweis

Sie können Standardwerte für ein Attribut aus anderen Attributen erzeugen, indem Sie statt eines absoluten Wertes eine Variablen-Schreibweise nutzen. Beispielsweise wird `cn=%sn %givenName` beim Anlegen eines Benutzers automatisch aus den Attributwerten von `sn` und `givenName` erzeugt.

Hinweis

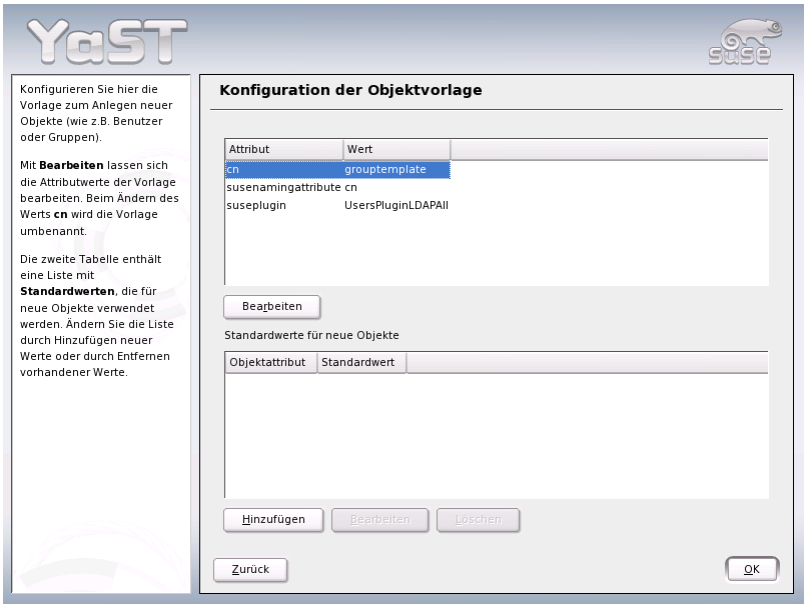

Abbildung 21.32: *YaST: Konfiguration eines Objekt-Templates*

Sind alle Module und Templates korrekt konfiguriert und einsatzbereit, erfassen Sie mit YaST wie gewohnt neue Gruppen und Benutzer.

Benutzer und Gruppen — Konfiguration mit YaST

Nachdem Module und Templates für das Netzwerk einmal konfiguriert worden sind, weicht die eigentliche Erfassung der Benutzer- und Gruppendaten nur geringfügig von der Vorgehensweise ohne LDAP-Verwendung ab. Die folgende Kurzanleitung bezieht sich auf die Verwaltung von Benutzern, das Vorgehen für die Verwaltung von Gruppen ist analog.

Die YaST-Benutzerverwaltung erreichen Sie über ‘Sicherheit & Benutzer’ -> ‘Benutzer bearbeiten und anlegen’. Wollen Sie einen neuen Benutzer hinzufügen, klicken Sie auf den Button ‘Hinzufügen’. Sie gelangen in eine Eingabemaske zur Erfassung der wichtigsten Benutzerdaten wie Name, Login und Passwort. Nach Ausfüllen dieser Maske geht es über den Button ‘Details’ in eine Maske zur verfeinerten Konfiguration der Gruppenzugehörigkeit, Login-Shell und des Homeverzeichnisses. Die Voreinstellungen der Eingabefelder haben Sie nach dem unter Abschnitt 21.8.6 auf Seite 545

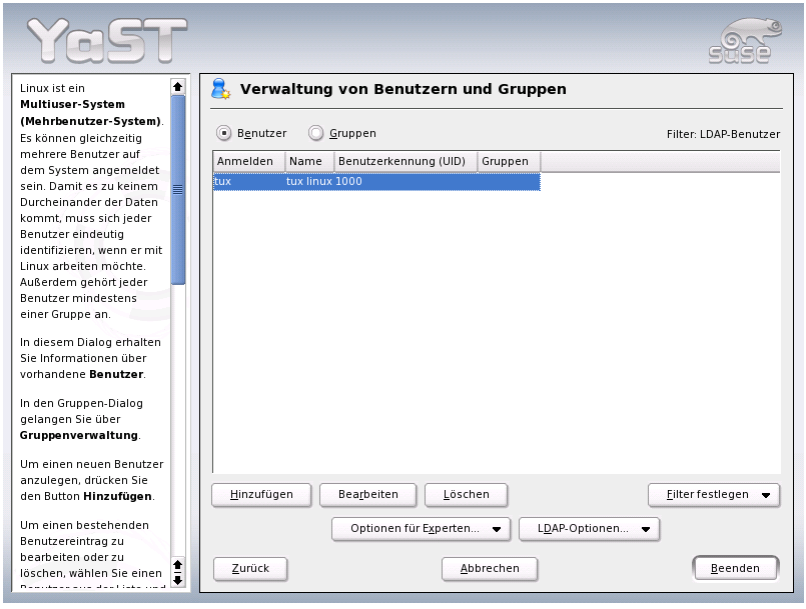

Abbildung 21.33: *YaST: Benutzerverwaltung*

beschriebenen Verfahren eingerichtet. Bei aktivierter LDAP-Verwendung gelangen Sie aus dieser Maske in eine weitere Maske zur Erfassung LDAP-spezifischer Attribute (siehe Abbildung 21.34 auf der nächsten Seite) . Selektieren Sie nach und nach alle Attribute, deren Wert Sie verändern möchten und klicken Sie auf 'Bearbeiten', um das entsprechende Eingabefenster zu öffnen. Verlassen Sie danach diese Maske über 'Weiter' und kehren Sie zur Startmaske der Benutzerverwaltung zurück.

Aus der Startmaske der Benutzerverwaltung (siehe Abbildung 21.33) heraus haben Sie über den Button 'LDAP-Optionen' die Möglichkeit, LDAP-Suchfilter auf die Menge der verfügbaren Benutzer anzuwenden oder über 'LDAP Benutzer- und Gruppenkonfiguration' in die Modulkonfiguration für LDAP-Benutzer und -gruppen zu gelangen.

21.8.7 Weitere Informationen

Komplexere Themen wie die SASL-Konfiguration oder das Aufsetzen eines replizierenden LDAP-Servers, der sich die Arbeit mit mehreren „slaves“

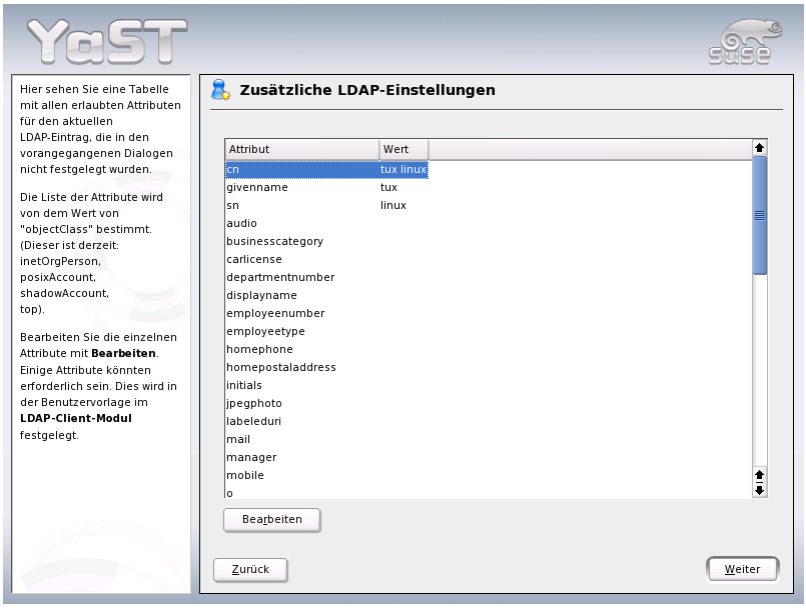

Abbildung 21.34: *YaST: Zusätzliche LDAP-Einstellungen*

teilt, wurden in diesem Kapitel bewusst ausgeklammert. Detaillierte Informationen zu beiden Themen finden Sie im *OpenLDAP 2.2 Administrator's Guide* (Links siehe unten).

Auf den Webseiten des OpenLDAP-Projekts stehen ausführliche Dokumentationen für Anfänger und fortgeschrittene LDAP-Benutzer bereit:

OpenLDAP Faq-O-Matic Eine sehr ergiebige Frage- und Antwortsammlung rund um Installation, Konfiguration und Benutzung von OpenLDAP: `http://www.openldap.org/faq/data/cache/1.html`

Quick Start Guide Eine knappe Schritt-für-Schritt-Anleitung zum ersten eigenen LDAP-Server: `http://www.openldap.org/doc/admin22/quickstart.html` oder im installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`.

OpenLDAP 2.2 Administrator's Guide
Eine ausführliche Einführung in alle wichtigen Bereiche der

LDAP-Konfiguration inkl. Access Controls und Verschlüsselung: `http://www.openldap.org/doc/admin22/` oder im installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`

Weiterhin beschäftigen sich folgende Redbooks von IBM mit dem Thema LDAP:

Understanding LDAP Eine sehr ausführliche, allgemeine Einführung in die Grundprinzipien von LDAP: `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`

LDAP Implementation Cookbook
Zielgruppe sind speziell Administratoren von *IBM SecureWay Directory*. Jedoch sind auch wichtige allgemeine Informationen zum Thema LDAP enthalten: `http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf`

Gedruckte, englischsprachige Literatur zu LDAP:

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2. Aufl., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Ultimative Nachschlagewerke zum Thema LDAP sind die entsprechenden RFCs (engl. *Request for comments*) 2251 bis 2256.

21.9 NIS – Network Information Service

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen wollen, muss sichergestellt sein, dass Benutzer- und Gruppenkennungen auf allen Rechnern miteinander harmonieren. Das Netzwerk soll für den Anwender transparent sein. Egal welcher Rechner, der Anwender findet immer die gleiche Umgebung vor. Möglich wird dies durch die Dienste NIS und NFS. NFS dient der Verteilung von Dateisystemen im Netz und wird in Abschnitt 21.10 auf Seite 557 beschrieben.

NIS (engl. *Network Information Service*) kann als Datenbankdienst verstanden werden, der Zugriff auf Informationen aus den Dateien `/etc/`

passwd, /etc/shadow oder /etc/group netzwerkweit ermöglicht. NIS kann auch für weitergehende Aufgaben eingesetzt werden (zum Beispiel für /etc/hosts oder /etc/services). Darauf soll hier jedoch nicht im Detail eingegangen werden. Für NIS wird vielfach synonym der Begriff *YP* verwendet. Dieser leitet sich ab von den *yellow pages*, also den *gelben Seiten* im Netz.

21.9.1 NIS Master und Slave Server

Zur Konfiguration wählen Sie in YaST 'Netzwerkdienste' und dort 'NIS-Server'. Wenn in Ihrem Netzwerk bisher noch kein NIS-Server existiert, müssen Sie in der nächsten Maske den Punkt 'NIS Master Server installieren und einrichten' aktivieren. Falls Sie schon einen NIS-Server (also einen „Master") haben, können Sie (beispielsweise wenn Sie ein neues Subnetz einrichten) einen NIS Slave-Server hinzufügen. Zunächst wird die Konfiguration des Master-Servers erläutert. Falls nicht alle nötigen Pakete installiert sind, wird YaST Sie auffordern, die entsprechende CD oder DVD einzulegen, damit die Pakete automatisch nachinstalliert werden. In der ersten Konfigurationsmaske (Abbildung 21.35 auf der nächsten Seite) geben Sie oben den Domainnamen ein. In der Checkbox darunter können Sie festlegen, ob der Rechner auch ein NIS-Client werden soll, also ob sich darauf auch Benutzer einloggen können, die dann ebenfalls die Daten vom NIS-Server erhalten.

Wollen Sie zusätzliche NIS-Server („Slave-Server") in Ihrem Netzwerk einrichten, müssen Sie die Box 'Aktiver Slave-Server für NIS vorhanden' aktivieren. Zusätzlich sollten Sie dann auch die 'Schnelle Map-Verteilung' aktivieren, die bewirkt, dass die Datenbankeinträge sehr schnell vom Master auf die Slave-Server übertragen werden.

Wollen Sie den Nutzern in Ihrem Netzwerk erlauben, dass sie ihre Passwörter ändern können (mit dem Befehl yppasswd, also nicht nur die lokalen, sondern die, die auf dem NIS-Server abgelegt sind), können Sie das hier ebenfalls aktivieren. Dann werden auch die Checkboxen 'Ändern des GECOS-Eintrags zulassen' und 'Ändern des SHELL-Eintrags zulassen' aktiv. „GECOS" bedeutet, der User kann auch seine Namens- und Adresseinstellungen ändern (mit dem Befehl ypchfn). „SHELL" heisst, er darf auch seine standardmäßig eingetragene Shell ändern (mit dem Befehl ypchsh, zum Beispiel von bash zu sh).

Durch Klick auf 'Andere globale Einstellungen...' gelangen Sie in einen Dialog (Abb. 21.36 auf Seite 556), in dem man das Quellverzeichnis des NIS-Servers (standardmäßig /etc/) ändern kann. Zusätzlich kann man

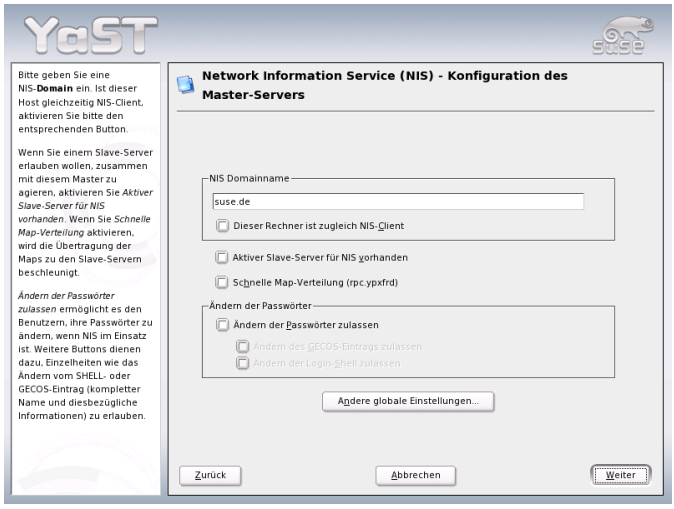

Abbildung 21.35: *YaST: NIS-Server Konfigurationstool*

hier noch Passwörter und Gruppen zusammenführen. Die Einstellung sollte man auf ‘Ja’ belassen, damit die jeweiligen Dateien (`/etc/passwd` und `/etc/shadow` bzw. `/etc/group`) aufeinander abgestimmt werden. Zusätzlich kann noch die jeweils kleinste Benutzer- und Gruppenkennummer festgelegt werden. Mit ‘OK’ bestätigen Sie Ihre Eingaben und gelangen wieder in die vorige Maske zurück. Klicken Sie hier auf ‘Weiter’.

Haben Sie vorher ‘Aktiver Slave-Server für NIS vorhanden’ aktiviert, müssen Sie nun die Namen der Rechner angeben, die als Slaves fungieren sollen. Anschließend klicken Sie auf ‘Weiter’. Werden keine Slave-Server benutzt, belangen Sie direkt zum Dialog für die Datenbank-Einstellungen. Hier geben Sie die „Maps“ an, das heißt die Teildatenbanken, die vom NIS-Server auf den jeweiligen Client übertragen werden sollen. Die Voreinstellungen hier sind für die meisten Fälle sehr sinnvoll. Daher sollten Sie im Normalfall nichts ändern.

Mit ‘Weiter’ gelangen Sie in den letzten Dialog. Legen Sie fest, aus welchen Netzwerken Anfragen an den NIS-Server gestellt werden dürfen (siehe Abb. 21.37 auf Seite 557). Normalerweise wird das Ihr Firmennetzwerk sein. Dann sollten die folgenden beiden Einträge hier stehen:

```
255.0.0.0 127.0.0.0
0.0.0.0   0.0.0.0
```

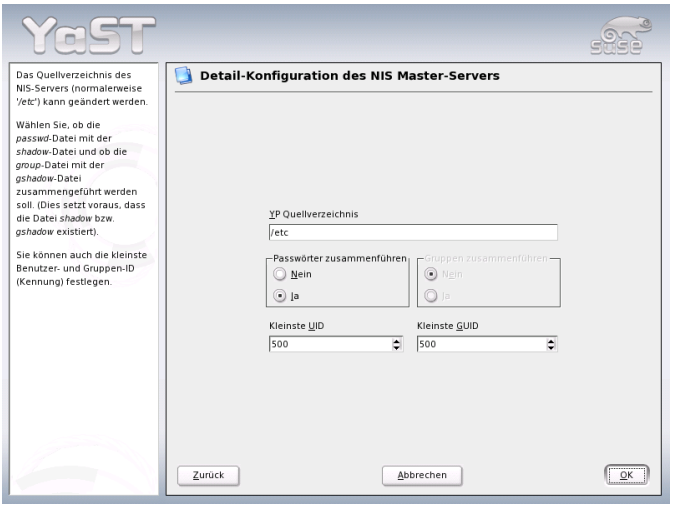

Abbildung 21.36: *YaST: NIS-Server: Verzeichnis ändern und Dateien synchronisieren*

Der erste erlaubt Verbindungen vom eigenen Rechner, der zweite ermöglicht allen Rechnern, die Zugriff auf das Netzwerk haben, Anfragen an den Server.

21.9.2 Das NIS-Client-Modul in YaST

Mit diesem Modul können Sie sehr einfach den NIS-Client konfigurieren. Nachdem Sie sich in der Startmaske für die Verwendung von NIS und unter Umständen des Automounters entschieden haben, gelangen Sie in die nächste Maske. Geben Sie hier an, ob der NIS-Client eine statische IP-Adresse hat oder ob er diese über DHCP erhalten soll. In letzterem Fall können Sie keine NIS-Domain oder IP-Adresse des Servers angeben, da diese Daten ebenfalls über DHCP zugewiesen werden. Weitere Information zu DHCP finden Sie im Abschnitt 21.11 auf Seite 563. Falls der Client über eine feste IP-Adresse verfügt, müssen NIS-Domain und -Server manuell eingetragen werden (siehe Abbildung 21.38 auf Seite 558) . Über den Button 'Suchen' kann YaST nach einem aktiven NIS-Server in Ihrem Netz suchen.

Sie haben auch die Möglichkeit, multiple Domains mit einer Default-

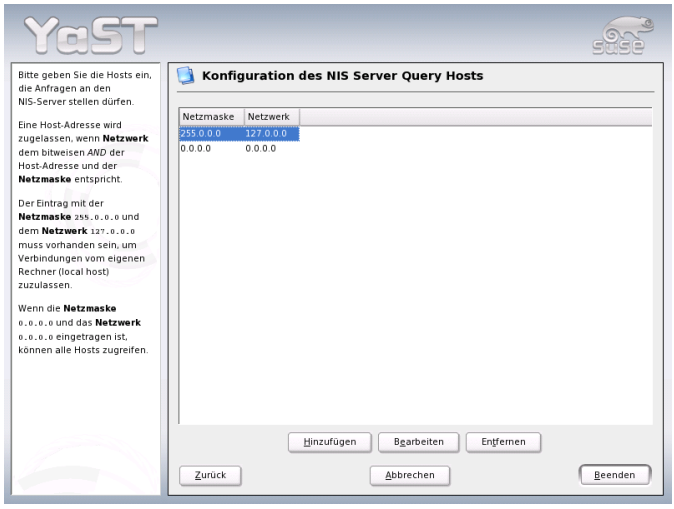

Abbildung 21.37: *YaST: NIS-Server: Festlegen der Anfrage-Erlaubnis*

Domain anzugeben. Für die einzelnen Domains können Sie wiederum mit ‘Hinzufügen’ mehrere Server einschließlich Broadcast-Funktion angeben.

In den Experten-Einstellungen können Sie verhindern, dass ein anderer Rechner im Netz abfragen kann, welchen Server Ihr Client benutzt. Wenn Sie ‘Broken Server’ aktivieren, werden auch Antworten von einem Server auf einem unprivilegierten Port akzeptiert. Details dazu finden Sie in der Manual-Page von `ypbind`.

21.10 NFS – verteilte Dateisysteme

Wie bereits in Abschnitt 21.9 auf Seite 553 erwähnt, dient NFS neben NIS dazu, ein Netzwerk für Anwender transparent zu machen. Durch NFS lassen sich Dateisysteme im Netz verteilen. Unabhängig davon, an welchem Rechner im Netz ein Anwender arbeitet, findet er so stets die gleiche Umgebung vor.

Wie NIS ist auch NFS ein asymmetrischer Dienst. Es gibt NFS–Server und NFS–Clients. Allerdings kann ein Rechner beides sein, d.h. gleichzeitig Dateisysteme dem Netz zur Verfügung stellen („exportieren“) und Dateisysteme anderer Rechner mounten („importieren“). Im Regelfall jedoch

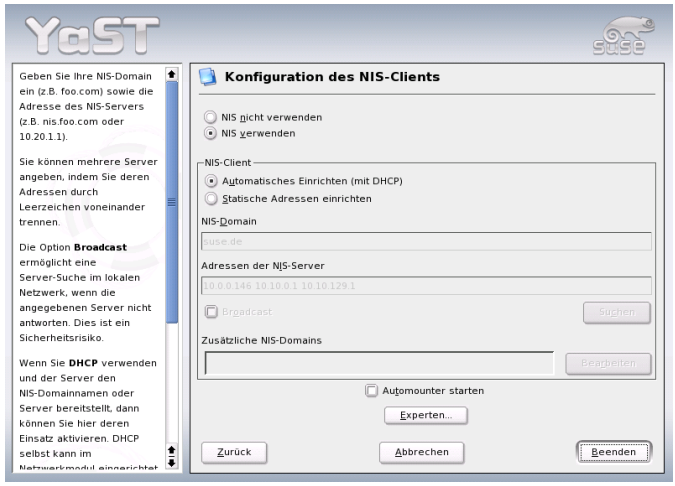

Abbildung 21.38: *Angabe von Domain und Adresse des NIS-Servers*

benutzt man dafür Server mit großer Festplattenkapazität, deren Dateisysteme von Clients gemountet werden.

21.10.1 Importieren von Dateisystemen mit YaST

Jeder Benutzer (der die Rechte dazu erteilt bekommt), kann NFS-Verzeichnisse von NFS-Servern in seinen eigenen Dateibaum einhängen. Dies lässt sich am einfachsten mit dem Modul 'NFS-Client' in YaST erledigen. Dort muss lediglich der Hostname des als NFS-Server fungierenden Rechners eingetragen werden, das Verzeichnis, das von dem Server exportiert wird und den Mountpunkt, unter dem es auf dem eigenen Computer eingehängt werden soll. Wählen Sie dazu im ersten Dialogfenster 'Hinzufügen' und tragen Sie dann die genannten Angaben ein (s. Abb. 21.39 auf der nächsten Seite).

21.10.2 Manuelles Importieren von Dateisystemen

Dateisysteme von einem NFS–Server manuell zu importieren, ist sehr einfach. Einzige Voraussetzung ist, dass der RPC–Portmapper läuft. Das Starten erledigen Sie durch Aufruf des Befehls `rcportmap start` als Benutzer

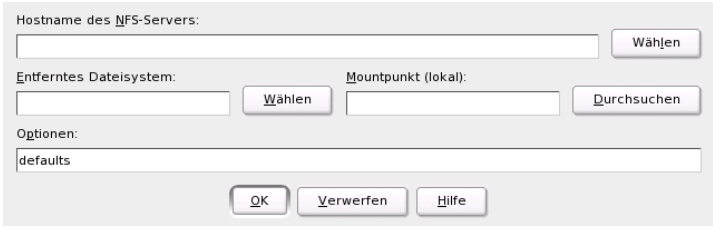

Abbildung 21.39: *Konfiguration des NFS-Clients*

`root`. Ist diese Voraussetzung erfüllt, können fremde Dateisysteme, sofern sie von den entsprechenden Maschinen exportiert werden, analog zu lokalen Platten mit dem Befehl `mount` in das Dateisystem eingebunden werden. Die Syntax ist wie folgt:

```
mount Rechner:Remote-Pfad Lokaler-Pfad
```

Sollen also z.B. die Benutzerverzeichnisse vom Rechner sun importiert werden, so kann dies mit folgendem Befehl erreicht werden:

```
mount sun:/home /home
```

21.10.3 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Rechner Ihres Netzwerks zu einem NFS-Server machen. Das ist ein Server, der Verzeichnisse und Dateien für alle Rechner, denen Sie Zugang gewähren, bereitstellt. Viele Anwendungsprogramme können so z.B. für Mitarbeiter zur Verfügung gestellt werden, ohne dass sie lokal auf deren Rechnern installiert werden müssen.

Zur Installation wählen Sie in YaST ‘Netzwerkdienste’ und dort ‘NFS-Server’ (Abb. 21.40 auf der nächsten Seite).

Im nächsten Schritt aktivieren Sie ‘NFS-Server starten’ und klicken auf ‘Weiter’. Jetzt ist nur noch ein Schritt zu tun: Sie müssen im oberen Feld die Verzeichnisse eintragen, die exportiert werden sollen und im unteren die Rechner Ihres Netzwerks, die darauf Zugriff erhalten (Abb. 21.41 auf Seite 561). Zu den Rechnern sind jeweils vier Optionen einstellbar, `single host`, `netgroups`, `wildcards` und `IP networks`. Nähere Erläuterungen zu diesen Optionen finden Sie in den Man-Pages zu `exports`.

Mit ‘Beenden’ schließen Sie die Konfiguration ab.

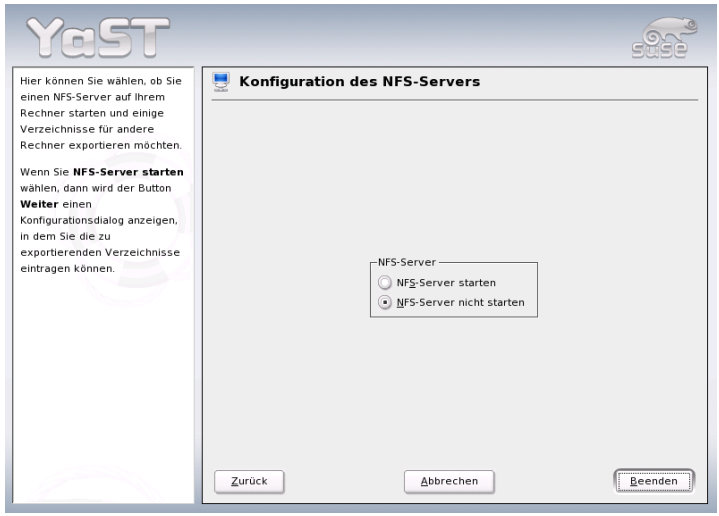

Abbildung 21.40: *NFS-Server Konfigurationstool*

21.10.4 Manuelles Exportieren von Dateisystemen

Wenn Sie auf die Unterstützung durch YaST verzichten, müssen Sie dafür sorgen, dass die folgenden Dienste auf dem NFS-Server laufen:

- RPC-Portmapper (portmap)
- RPC-Mount-Daemon (rpc.mountd)
- RPC-NFS-Daemon (rpc.nfsd)

Damit diese beim Hochfahren des Systems von den Skripten `/etc/init.d/portmap` und `/etc/init.d/nfsserver` gestartet werden, geben Sie bitte die Befehle `insserv /etc/init.d/nfsserver` und `insserv /etc/init.d/portmap` ein.

Neben dem Start dieser Daemonen muss noch festgelegt werden, welche Dateisysteme an welche Rechner exportiert werden sollen. Dies geschieht in der Datei `/etc/exports`.

Je Verzeichnis, das exportiert werden soll, wird eine Zeile für die Information benötigt, welche Rechner wie darauf zugreifen dürfen. Alle Unterverzeichnisse eines exportierten Verzeichnisses werden ebenfalls automatisch

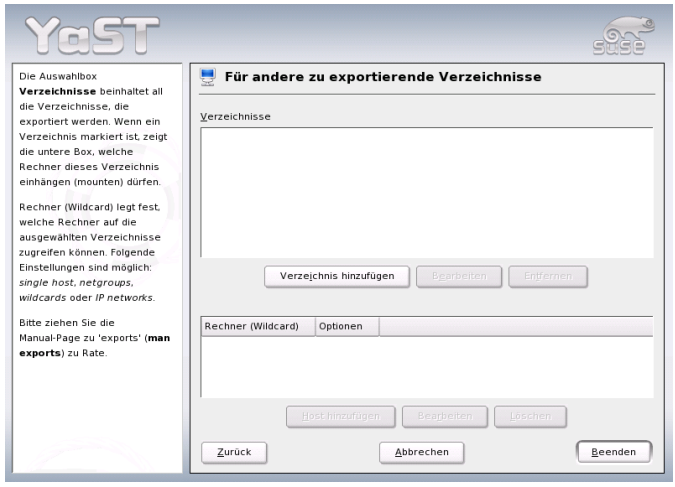

Abbildung 21.41: *NFS-Server: Exportverzeichnisse und Hosts eintragen*

exportiert. Die berechtigten Rechner werden üblicherweise mit ihren Namen (inklusive Domainname) angegeben, es ist aber auch möglich, mit den Jokerzeichen * und ? zu arbeiten, die die aus der bash bekannte Funktion haben. Wird kein Rechnername angegeben, hat jeder Rechner die Erlaubnis, auf dieses Verzeichnis (mit den angegebenen Rechten) zuzugreifen.

Die Rechte, mit denen das Verzeichnis exportiert wird, werden in einer von Klammern umgebenen Liste nach dem Rechnernamen angegeben. Die wichtigsten Optionen für die Zugriffsrechte sind in der folgenden Tabelle beschrieben.

Tabelle 21.12: *Zugriffsrechte für exportierte Verzeichnisse*

Optionen	Bedeutung
`ro`	Dateisystem wird nur mit Leserechten exportiert (Vorgabe).
`rw`	Dateisystem wird mit Schreib- und Leserechten exportiert.

`root_squash`	Diese Option bewirkt, dass der Benutzer `root` des angegebenen Rechners keine für `root` typischen Sonderrechte auf diesem Dateisystem hat. Erreicht wird dies, indem Zugriffe mit der User–ID `0` auf die User–ID `65534 (-2)` umgesetzt werden. Diese User-ID sollte dem Benutzer `nobody` zugewiesen sein (Vorgabe).
`no_root_squash`	Rootzugriffe nicht umsetzen; Root-rechte bleiben also erhalten.
`link_relative`	Umsetzen von absoluten, symbolischen Links (solche, die mit `/` beginnen) in eine entsprechende Folge von `../`. Diese Option ist nur dann sinnvoll, wenn das gesamte Dateisystem eines Rechners gemountet wird (Vorgabe).
`link_absolute`	Symbolische Links bleiben unverändert.
`map_identity`	Auf dem Client werden die gleichen User–IDs wie auf dem Server verwendet (Vorgabe).
`map_daemon`	Client und Server haben keine übereinstimmenden User–IDs. Durch diese Option wird der nfsd angewiesen, eine Umsetztabelle für die User–IDs zu erstellen. Voraussetzung dafür ist jedoch die Aktivierung des Daemons **ugidd**.

Die `exports`–Datei kann beispielsweise aussehen wie Datei 21.29.

Beispiel 21.29: */etc/exports*

```
#
# /etc/exports
#
/home            sonne(rw)   venus(rw)
/usr/X11         sonne(ro)   venus(ro)
/usr/lib/texmf   sonne(ro)   venus(rw)
/                erde(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

Die Datei `/etc/exports` wird von mountd und nfsd gelesen. Wird also eine Änderung daran vorgenommen, so müssen mountd und nfsd neu

gestartet werden, damit diese Änderung berücksichtigt wird! Erreicht wird dies am einfachsten mit dem Befehl:

```
rcnfsserver restart
```

21.11 DHCP

21.11.1 Das DHCP-Protokoll

Hinweis

S/390, zSeries: DHCP-Unterstützung

Lediglich Karten vom Typ OSA und OSA Express bieten unter IBM S/390 und zSeries DHCP-Unterstützung, da sie eine MAC-Adresse haben, die von DHCP als Anhaltspunkt für die automatische Konfiguration verwendet werden kann.

Hinweis

Das „Dynamic Host Configuration Protocol“ dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zu vergeben. Einstellungen müssen also nicht dezentral an einzelnen Arbeitsplatzrechnern konfiguriert werden. Ein mit DHCP konfigurierter Client verfügt selbst nicht über statische Adressen, sondern konfiguriert sich voll und ganz selbstständig nach den Vorgaben des DHCP-Servers.

Dabei ist es möglich, jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte zu identifizieren und ständig mit denselben Einstellungen zu versorgen, sowie Adressen aus einem dafür bestimmten Pool „dynamisch“ an jeden „interessierten“ Rechner zu vergeben. In diesem Fall wird sich der DHCP-Server bemühen, jedem Client bei jeder Anforderung (auch über einen längeren Zeitraum hinweg) dieselbe Adresse zuzuweisen — dies funktioniert natürlich nicht, wenn es mehr Rechner im Netz als Adressen gibt.

Ein Systemadministrator kann somit gleich in zweierlei Hinsicht von DHCP profitieren. Einerseits ist es möglich, selbst umfangreiche Änderungen der Netzwerk-Adressen oder der Konfiguration komfortabel in der Konfigurationsdatei des DHCP-Servers zentral vorzunehmen, ohne dass eine Vielzahl von Clients einzeln konfiguriert werden müssen. Andererseits

können vor allem neue Rechner sehr einfach ins Netzwerk integriert werden, indem sie aus dem Adress-Pool eine IP-Nummer zugewiesen bekommen. Auch für Laptops, die regelmäßig in verschiedenen Netzen betrieben werden, ist die Möglichkeit, von einem DHCP-Server jeweils passende Netzwerkeinstellungen zu beziehen, sicherlich interessant.

Neben IP-Adresse und Netzmaske werden der Rechner- und Domain-Name, der zu verwendende Gateway und Nameserver-Adressen dem Client mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, zum Beispiel ein Zeitserver, von dem die jeweils aktuelle Uhrzeit abrufbar ist oder ein Druckserver. Im Folgenden möchten wir Ihnen nun einen kurzen Einblick in die Welt von DHCP geben. Wir möchten Ihnen anhand des DHCP-Servers dhcpd zeigen, wie einfach auch in Ihrem Netzwerk die gesamte Netzwerkkonfiguration zentral per DHCP erledigt werden kann.

21.11.2 DHCP-Softwarepakete

Bei SUSE LINUX stehen Ihnen sowohl ein DHCP-Server-, als auch zwei Client-Pakete zur Verfügung. Der vom Internet Software Consortium herausgegebene DHCP-Server dhcpd stellt die Server-Funktionalität zur Verfügung, als Clients können sowohl der vom ISC herausgegebene dhclient als auch der so genannte „DHCP Client Daemon“ im Paket `dhcpcd` verwendet werden.

Der bei SUSE LINUX standardmäßig installierte dhcpcd ist sehr einfach zu handhaben und wird beim Starten des Rechners automatisch gestartet, um nach einem DHCP-Server zu suchen. Er kommt ohne eine Konfigurationsdatei aus und sollte im Normalfall ohne weitere Konfiguration funktionieren.

Für komplexere Situationen kann man auf den ISC dhclient zurückgreifen, der sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

21.11.3 Der DHCP-Server dhcpd

Der *Dynamic Host Configuration Protocol Daemon* ist das Herz eines DHCP-Systems. Er „vermietet“ Adressen und wacht über deren Nutzung, wie in der Konfigurationsdatei `/etc/dhcpd.conf` festgelegt. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des DHCP nach seinen Wünschen zu beeinflussen.

Ein Beispiel für eine einfache `/etc/dhcpd.conf`-Datei:

Beispiel 21.30: *Die Konfigurationsdatei /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "kosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Diese einfache Konfigurationsdatei reicht bereits aus, damit DHCP im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Strichpunkte am Ende jeder Zeile, ohne die dhcpd nicht starten wird!

Wie Sie sehen, lässt sich obige Beispieldatei in drei Blöcke unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Rechner „vermietet“ wird, bevor sich dieser um eine Verlängerung bemühen sollte (`default-lease-time`). Auch wird hier angegeben, wie lange ein Rechner maximal eine vom DHCP-Server vergebene IP-Nummer behalten darf, ohne für diese eine Verlängerung zu beantragen (`max-lease-time`).

Im zweiten Block werden nun einige grundsätzliche Netzwerk-Parameter global festgesetzt:

- Mit `option domain-name` wird die Default-Domain Ihres Netzwerks definiert.
- Bei `option domain-name-servers` können bis zu drei DNS-Server angegeben werden, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollte auf Ihrem System bzw. innerhalb Ihres Netzwerks ein Nameserver bereits in Betrieb sein, der auch für dynamische Adressen jeweils einen Hostnamen und umgekehrt bereit hält. Mehr über die Einrichtung eines eigenen Nameservers erfahren Sie in Abschnitt 21.7 auf Seite 502.

- `option broadcast-address` legt fest, welche Broadcast-Adresse der anfragende Rechner verwenden soll.
- `option routers` definiert, wohin Datenpakete geschickt werden können , die (aufgrund der Adresse von Quell- und Zielhost sowie Subnetz-Maske) nicht im lokalen Netz zugestellt werden können. Gerade bei kleineren Netzen ist dieser Router auch meist der Übergang zum Internet.
- `option subnet-mask` gibt die an den Client zu übergebende Netzmaske an.

Unterhalb dieser allgemeinen Einstellungen wird nun noch ein Netzwerk samt Subnet Mask definiert. Abschließend muss noch ein Bereich gewählt werden, aus dem der DHCP-Daemon Adressen an anfragende Clients vergeben darf. Im Beispiel stehen alle Adressen zwischen `192.168.1.10` und `192.168.1.20` bzw. `192.168.1.100` und `192.168.1.200` zur Verfügung.

Nach diesen wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Kommando `rcdhcpd start` zu aktivieren, der sogleich zur Verfügung steht.

Bei SUSE LINUX wird der DHCP-Daemon aus Sicherheitsgründen per default in einer chroot-Umgebung gestartet. Damit die Konfigurationsdateien gefunden werden, müssen diese mit in die neue Umgebung kopiert werden. Dies geschieht mit dem Befehl `rcdhcpd start` automatisch.

Auch können Sie mit `rcdhcpd check-syntax` eine kurze, formale Überprüfung der Konfigurationsdatei vornehmen lassen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten und der Server mit einem Fehler abbrechen und nicht mit einem „done“ starten, finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (Strg + Alt + F10).

21.11.4 Rechner mit fester IP-Adresse

Wie eingangs bereits erwähnt, kann mit DHCP auch an ein- und denselben Rechner bei jeder Anfrage eine ganz bestimmte, definierte Adresse vergeben werden.

Selbstverständlich haben solche expliziten Adresszuweisungen Vorrang vor solchen aus dem Pool der dynamischen Adressen. Im Gegensatz zu diesen verfallen die festen Adressinformationen in keinem Fall, wie es bei

den dynamischen der Fall ist, wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung erforderlich ist.

Zur Identifizierung eines mit einer *statischen* Adresse definierten Systems, bedient sich der dhcpd der so genannten Hardwareadresse. Dies ist eine weltweit i.d.R. einmalige, fest definierte Nummer aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, zum Beispiel `00:00:45:12:EE:F4`.

Wird nun die Konfigurationsdatei aus Datei 21.30 auf Seite 565 um einen entsprechenden Eintrag wie in Datei 21.31 ergänzt, wird dhcpd unter allen Umständen dieselben Daten an den entsprechenden Rechner ausliefern.

Beispiel 21.31: *Ergänzungen zur Konfigurationsdatei*

```
host erde {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

Der Aufbau dieser Zeilen ist nahezu selbsterklärend:

Zuerst wird der Name des zu definierenden Rechners eingetragen (`host` <hostname>) und in der folgenden Zeile die MAC-Adresse angegeben. Diese Adresse kann bei Linux-Rechnern mit dem Befehl ifstatus plus Netzwerkdevice (zum Beispiel `eth0`) festgestellt werden. Gegebenenfalls müssen Sie zuvor die Karte aktivieren: `ifup eth0`. Sie erhalten dann eine Ausgabe wie:

```
link/ether 00:00:45:12:EE:F4
```

In unserem Beispiel wird also dem Rechner, dessen Netzwerkkarte die MAC-Adresse `00:00:45:12:EE:F4` hat, die IP-Adresse `192.168.1.21` sowie der Rechnername `erde` zugewiesen.

Als Hardware-Typ wird heutzutage in aller Regel `ethernet` zum Einsatz kommen, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

21.11.5 Besonderheiten bei SUSE LINUX

Aus Sicherheitsgründen enthält bei SUSE LINUX der ISC DHCP-Server den 'non-root/chroot'-Patch von Ari Edelkind. Damit kann der dhcpd als User `nobody` und in einer „chroot"-Umgebung (`/var/lib/dhcp/`) laufen.

Die Konfigurationsdatei `/etc/dhcpd.conf` muss dafür in `/var/lib/dhcp/etc/` liegen, und wird vom Init-Skript beim Start automatisch dorthin kopiert.

Dieses Verhalten lässt sich in der Datei `/etc/sysconfig/dhcpd` steuern. Um den dhcpd weiterhin ohne chroot-Umgebung laufen zu lassen, setzen Sie in der Datei `/etc/sysconfig/dhcpd` die Variable `DHCPD_RUN_CHROOTED` auf „no"

Damit der dhcpd auch in der chroot-Umgebung Hostnamen auflösen kann, müssen einige weitere Konfigurationsdateien mit kopiert werden. Dies sind:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Beim Start des Init-Skriptes werden diese deshalb nach `/var/lib/dhcp/etc/` kopiert. Diese Dateien müssen auf dem Laufenden gehalten werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Wenn in der Konfigurationsdatei nur IP-Adressen anstelle von Hostnamen verwendet werden, sind keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien mit in die chroot-Umgebung kopiert werden müssen, so können Sie diese mit dem Parameter `DHCPD_CONF_INCLUDE_FILES` in der Datei `etc/sysconfig/dhcpd` angeben.

Damit der dhcp-Daemon aus der chroot-Umgebung heraus weiter protokollieren kann, auch wenn der Syslog-Daemon neu gestartet wird, muss zu der Variablen `SYSLOGD_PARAMS` in `/etc/sysconfig/syslog` der Parameter `"-a /var/lib/dhcp/dev/log"` hinzugefügt werden.

21.11.6 DHCP-Konfiguration mit YaST

Hinweis

LDAP-Unterstützung

Der YaST DHCP-Server unterstützt mit dieser Version des SUSE LINUX Enterprise Servers alternativ zu der lokalen Speicherung der Serverkonfiguration auf dem DHCP-Server selbst die Verwaltung der Konfigurationsdaten über LDAP.

Hinweis

Das YaST DHCP-Modul dient der Konfiguration eines eigenen DHCP-Servers im lokalen Netz. Dieses Modul kennt zwei verschiedene Funktionsweisen:

Initiale Konfiguration Beim ersten Start des Moduls werden von dem Administrator einige grundlegende Entscheidungen verlangt. Nach Abschluss der initialen Konfiguration ist der Server startklar und für einfache Szenarien ausreichend konfiguriert.

Experten-Konfiguration Der Expertenmodus dient komplexeren Konfigurationsaufgaben wie dynamischem DNS, TSIG-Verwaltung etc.

Hinweis

Navigation im Modul und Anzeige der Hilfetexte

Alle Dialoge des DHCP-Server-Moduls folgen einem ähnlichen Aufbauprinzip. Im linken Teilbereich des Dialogfensters ist eine Baumansicht zur Navigation durch die einzelnen Teilbereiche der Konfiguration angezeigt, während im rechten Bereich die eigentliche Dialogmaske angezeigt wird. Wünschen Sie einen Hilfetext zur aktuellen Dialogmaske, klicken Sie auf das Icon mit dem Rettungsring am linken unteren Bildrand. Um diese Hilfe zu verlassen und in die Baumansicht zurückzugelangen, klicken Sie auf das Icon mit der stilisierten Baumansicht.

Hinweis

Initiale Konfiguration

Beim ersten Start des Moduls ruft YaST einen vierteiligen Konfigurationsassistenten auf. Nach dessen Beendigung ist ein einfacher DHCP-Server in Ihrem Netz einsatzbereit.

Auswahl der Netzwerkschnittstelle
Im ersten Schritt ermittelt YaST die in Ihr System eingebundenen Netzwerkschnittstellen. Wählen Sie aus der angebotenen Liste diejenige aus, auf der der DHCP-Server lauschen soll (siehe Abb. 21.42).

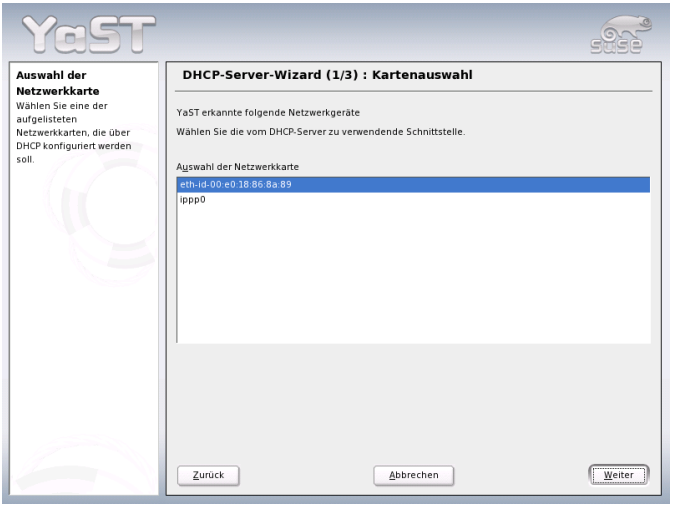

Abbildung 21.42: *DHCP-Server: Auswahl der Netzwerkschnittstelle*

Globale Einstellungen Per Checkox legen Sie fest, ob Ihre DHCP-Einstellungen automatisch auf einem LDAP-Server gespeichert werden sollen. In den weiteren Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Dies sind: Name der Domain, Adresse des Zeitservers, Adresse des primären und sekundären Nameservers, Adresse des Druckservers und WINS-Servers (im gemischten Einsatz von Windows- und Linux-Clients) sowie Adresse des Gateways und Leasing-Zeitraum (siehe Abb. 21.43 auf der nächsten Seite).

DHCP-Server: Dynamisches DCHP
In diesem Schritt konfigurieren Sie die dynamische IP-Vergabe an angeschlossene Clients. Hierzu legen Sie eine Spanne von IP-Adressen fest, innerhalb derer die zu vergebenden Adressen liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend den Leasing-Zeitraum fest, für den ein Client eine Adresse behalten darf, ohne eine Anfrage um

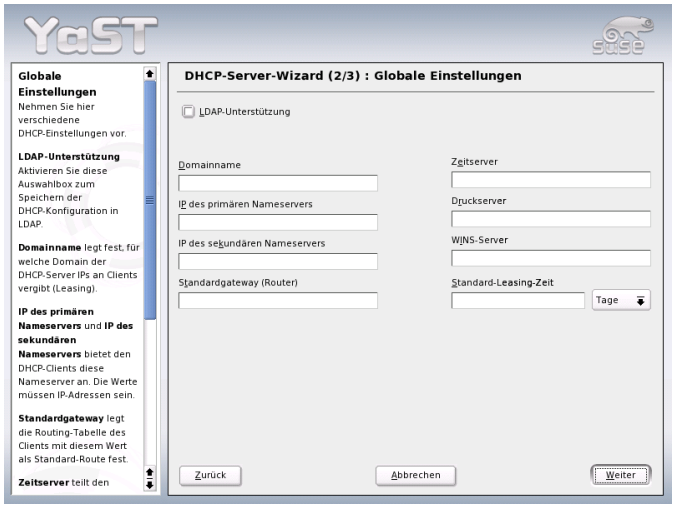

Abbildung 21.43: *DHCP-Server: Globale Einstellungen*

Verlängerung des Leasing-Zeitraumes zu „beantragen“. Des Weiteren setzen Sie optional den maximalen Leasing-Zeitraum fest, für den eine bestimmte IP-Adresse auf dem Server für einen bestimmten Client reserviert bleibt (siehe Abbildung 21.44 auf der nächsten Seite).

Abschluss der Konfiguration und Wahl des Startmodus
Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in einen letzten Dialog, der sich mit den Startoptionen des DHCP-Servers befasst. ‘An’ bewirkt, dass bei jedem Hochfahren des Systems der DHCP-Server automatisch mit gestartet wird. ‘Aus’ bedeutet, dass der Server manuell gestartet werden muss. Klicken Sie auf ‘OK’, um die Konfiguration des Servers abzuschließen. Alternativ können Sie über die Baumstruktur am linken Rand des Dialogfensters den Punkt ‘Host-Verwaltung’ selektieren, um zusätzlich zur Basiskonfiguration speziellen Host-Verwaltung zu konfigurieren (siehe Abb. 21.45 auf Seite 573).

Host-Verwaltung Im Gegensatz zum oben beschriebenen dynamischen DCHP können Sie auch eine quasi statische Adressvergabe konfigurieren. Sie bauen mit Hilfe der Eingabefelder im unteren Dialogbereich eine Liste der zu verwaltenden Hostrechner auf. Die hierzu nötigen Angaben sind: ‘Name’ und ‘IP-Adresse’, die der Host erhalten

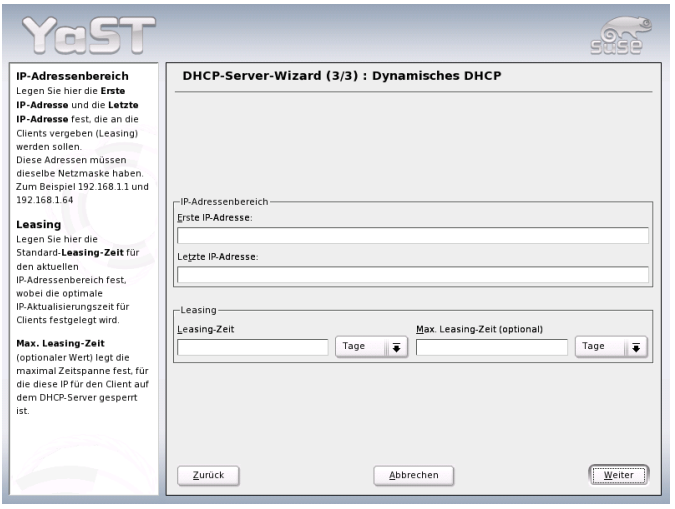

Abbildung 21.44: *DHCP-Server: Dynamisches DHCP*

soll, seine 'Hardware-Adresse' und 'Typ des Netzwerks' (Token Ring oder Ethernet). Über die Buttons 'Hinzufügen', 'Ändern' und 'Löschen' verwalten Sie die Liste der Hosts, die im oberen Dialogbereich angezeigt wird (siehe Abb. 21.45 auf der nächsten Seite).

Nachdem Sie den Konfigurationsassistenten vollständig durchlaufen und unter Umständen auch die zusätzliche Host-Verwaltung konfiguriert haben, verlassen Sie den letzten Dialog des Konfigurationsassistenten mit 'OK', um die Konfiguration zu übernehmen und den Server zu starten.

Experten-Konfiguration

Die Experten-Konfiguration erlaubt unabhängig von den beiden bereits beschriebenen Konfigurationsmodi sehr detaillierte Feineinstellungen an der DHCP-Server-Konfiguration. Der Expertenmodus wird gestartet, sobald Sie in der Baumansicht im linken Teilbereich des Dialogfensters den Punkt 'Einstellungen für Experten' selektieren.

Chroot-Betrieb und Deklarationen
Um die Konfiguration editierbar zu machen, klicken Sie in diesem ersten Dialog auf 'DHCP-Server starten'. Wichtiger Bestandteil des

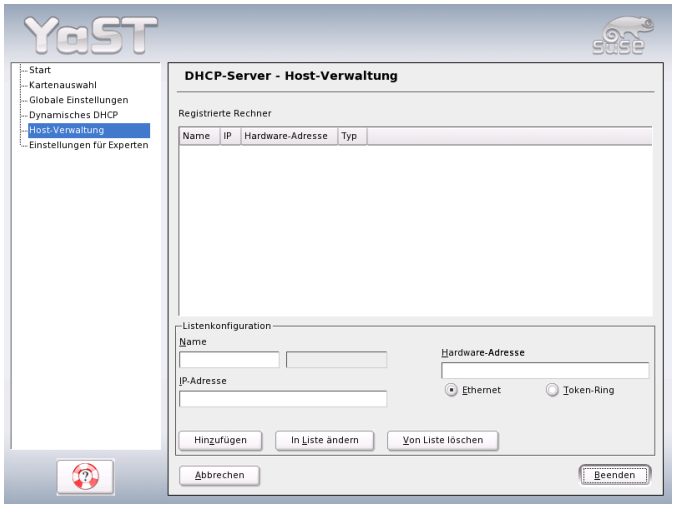

Abbildung 21.45: *DHCP-Server: Host-Verwaltung*

Startverhaltens des DHCP-Servers ist die Festlegung, ob der Server in einem *Chroot-Jail* gestartet wird oder nicht. Der Betrieb im Chroot-Jail dient der Absicherung des Serversystems. Wird der DHCP-Server durch einen Angriff von außen kompromittiert, ist das restliche System vor Kompromittierung sicher, da der Angreifer nicht aus der Chroot-Umgebung „ausbrechen“ kann. Im unteren Teil des Dialogs sehen Sie eine Baumansicht mit den bereits konfigurierten Deklarationen. Über ‘Hinzufügen’, ‘Löschen’ und ‘Bearbeiten’ können Sie diese Einstellungen beeinflussen. Über ‘Erweitert’ gelangen Sie in zusätzliche Expertendialoge (siehe Abb. 21.46 auf der nächsten Seite). Wählen Sie ‘Hinzufügen’, müssen Sie im folgenden Dialog den Typ der neuen Deklaration festlegen. Über den Button ‘Erweitert’ haben Sie die Möglichkeit, die Protokoll-Datei des Servers anzuschauen, die TSIG-Schlüssel-Verwaltung zu konfigurieren und die Firewallkonfiguration an die DHCP-Serverkonfiguration anzupassen.

Deklarationstyp wählen Die ‘globalen Optionen’ des DHCP-Servers setzen sich aus einer Reihe von so genannten Deklarationen zusammen. In diesem Dialog wählen Sie aus den Typen ‘Subnetz’, ‘Rechner’, ‘Gemeinsames Network’, ‘Gruppe’, ‘Adressen-Pool’, ‘Klasse’. Im Beispiel wählen Sie ein neues Subnetz (siehe Abb. 21.47 auf Seite 575).

Subnetz-Konfiguration Legen Sie das neue Subnetz mit IP-Adresse und Netzmaske fest. Der mittlere Teil des Dialogs dient dazu, die Optio-

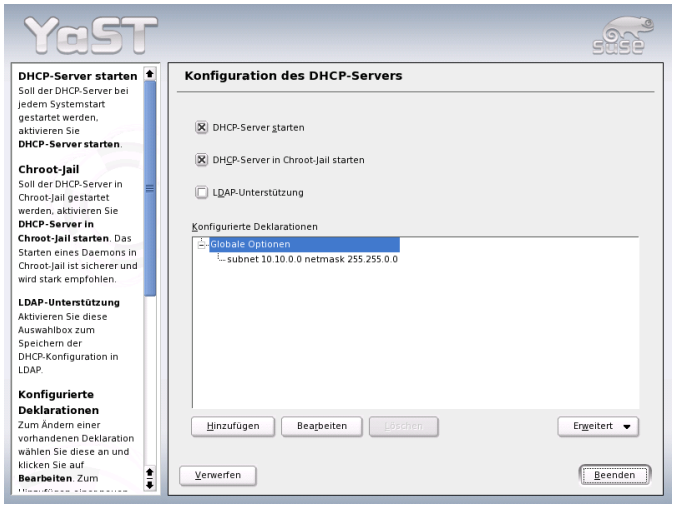

Abbildung 21.46: *DHCP-Server: Chroot-Jail und Deklarationen*

nen, mit denen der DHCP-Server für das gewählte Subnetz gestartet werden soll, zu konfigurieren. Diese können Sie über die Buttons 'Hinzufügen', 'Bearbeiten' und 'Löschen' bearbeiten. Wünschen Sie dynamisches DNS, klicken Sie auf den Button 'Dynamisches DNS'.

TSIG-Schlüssel-Verwaltung Haben Sie sich im oben beschriebenen Konfigurationsdialog für die Verwendung von dynamischem DNS (siehe hierzu auch Abschnitt 21.7.8 auf Seite 513) entschieden, konfigurieren Sie in diesem Dialog die Schlüssel-Verwaltung für den sicheren Zonentransfer (siehe Abb. 21.49 auf Seite 577. Mit 'OK' gelangen Sie in den Dialog zur Schnittstellenkonfiguration für dynamisches DNS (siehe Abb. 21.50 auf Seite 578).

Dynamisches DNS: Konfiguration der Schnittstelle
Aktivieren Sie für das neu zu konfigurierende Subnetz mit 'Dynamisches DNS für dieses Subnetz aktivieren' die Verwendung von dynamischem DNS. Anschließend wählen Sie mittels des Dropdown-Menüs die entsprechenden TSIG-Schlüssel für Forward- und Reverse-Zonen aus. Achten Sie dabei darauf, dass für die jeweiligen Schlüssel für DNS- und DHCP-Server gleich sind. Mit der Checkbox 'Globale dynamische DNS-Einstellungen aktualisieren' aktivieren Sie die automatische Aktualisierung und Anpassung der globalen

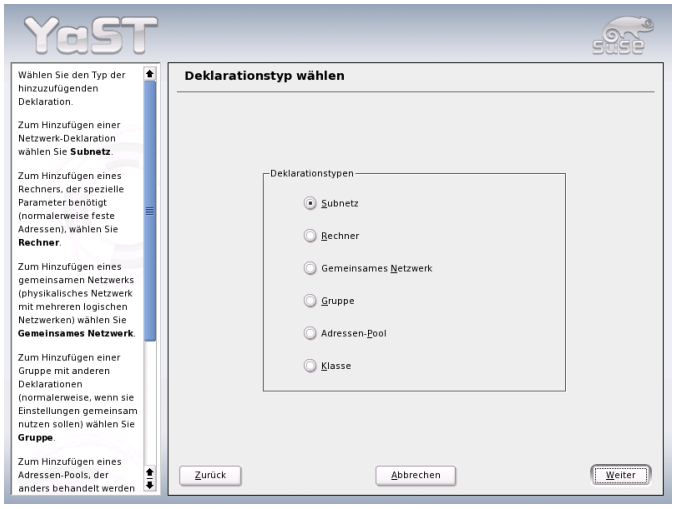

Abbildung 21.47: *DHCP-Server: Deklarationstypen*

Servereinstellungen des DHCP-Servers an dynamisches DNS. Abschließend geben Sie an, welche Forward- und Reverse-Zonen per dynamischem DNS aktualisiert werden sollen, und für jede der beiden Zonen jeweils den Namen des primären Nameservers. Läuft der Nameserver auf derselben Maschine wie der DHCP-Server, lassen Sie diese Eingabefelder leer. Mit ‘OK’ gelangen Sie zurück in den Dialog zur Konfiguration von Subnetzen (siehe Abb. 21.48 auf der nächsten Seite). Verlassen Sie diesen ebenfalls mit ‘OK’, gelangen Sie in den Ausgangsdialog der Experten-Konfiguration.

Konfiguration der Netzwerkschnittstelle

Aus dem Startdialog der Experten-Konfiguration gelangen Sie mit ‘Erweitert’ → ‘Konfiguration der Schnittstelle’ in den Dialog zur Festlegung der Schnittstellen, auf denen der DHCP-Server lauschen soll und zur Anpassung der Firewall-Konfiguration. Wählen Sie aus der Liste der von YaST angezeigten Schnittstellen, diejenige aus, auf denen der DHCP-Server lauschen soll. Um zu ermöglichen, dass aus allen Subnetzen Clients mit dem Server kommunizieren können, muss die vielleicht auf dem Server laufende Firewall angepasst werden. Markieren Sie hierfür die Checkbox ‘Firewall-Einstellungen anpassen’. YaST wird nun die Regeln der SuSEfirewall2 an die neuen

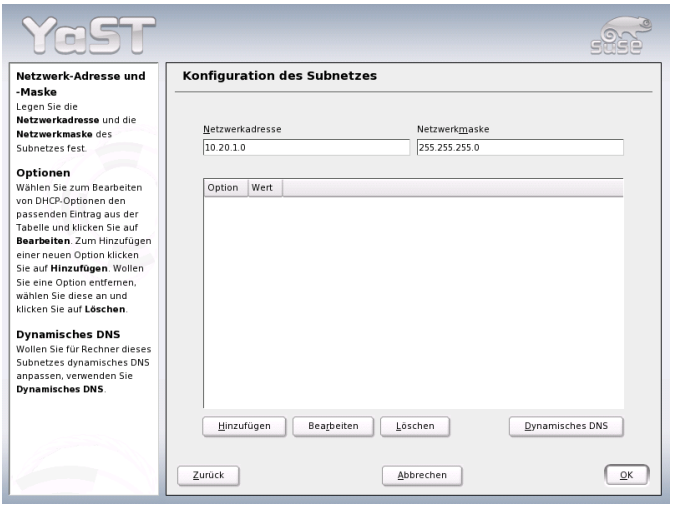

Abbildung 21.48: *DHCP-Server: Subnetze konfigurieren*

Gegebenheiten anpassen (siehe Abb. 21.51 auf Seite 579). ‘OK’ bringt Sie wieder in den Ausgangsdialog zurück.

Sind alle Konfigurationsschritte komplett durchlaufen, verlassen Sie den Experten-Dialog mit ‘OK’ und der Server startet mit der neuen Konfiguration.

21.11.7 Weitere Informationen

zusätzliche Informationen finden Sie zum Beispiel auf der Seite des *Internet Software Consortium* an, auf der detaillierte Informationen zu DHCP verfügbar sind: `http://www.isc.org/products/DHCP/`.

Auch die neue Version 3 des Protokolls, die sich im Moment im Beta-Test befindet, wird dort dokumentiert. Im Übrigen stehen selbstverständlich auch die Manpages zur Verfügung, dies sind insbesondere `man dhcpd`, `man dhcpd.conf`, `man dhcpd.leases` und `man dhcp-options`.

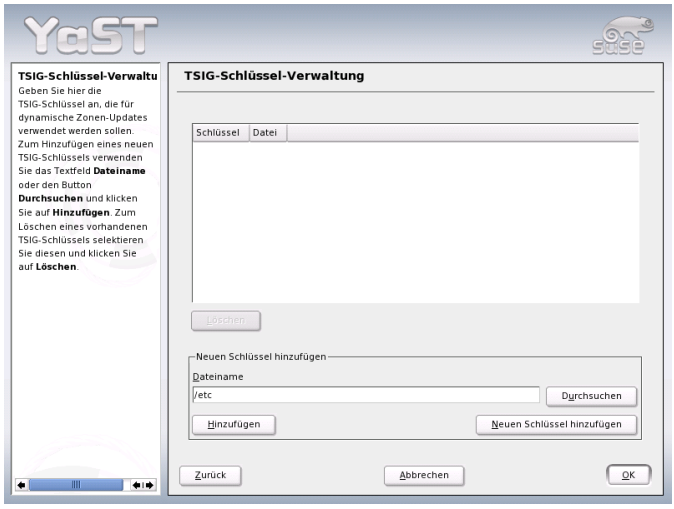

Abbildung 21.49: *DHCP-Server: TSIG-Konfiguration*

21.12 Zeitsynchronisation mit xntp

Bei vielen Abläufen in einem Computersystem spielt eine exakte Zeit eine wichtige Rolle. Zu diesem Zweck haben alle Rechner normalerweise eine Uhr eingebaut. Leider genügt diese oftmals nicht den Anforderungen, die von Applikationen wie Datenbanken gefordert werden. Man muss also die lokale Rechneruhr permanent nachstellen bzw. über ein Netzwerk korrigieren. Optimalerweise sollte eine Rechneruhr niemals rückwärts gestellt werden, und die Schritte, in denen sie nach vorne gestellt wird, sollten gewisse Zeitintervalle nicht überschreiten. Verhältnismäßig einfach ist es, die Rechneruhr mit ntpdate von Zeit zu Zeit nachzustellen. Dies bewirkt aber immer einen harten Sprung in der Zeit, der nicht von allen Anwendungen toleriert wird.

Einen interessanten Ansatz zur Lösung dieses Problems liefert xntp. Zum einen korrigiert xntp die lokale Rechneruhr laufend anhand von gesammelten Korrekturdaten und zum anderen korrigiert es kontinuierlich die lokale Zeit mit Hilfe von Zeitservern im Netz. Als dritte Möglichkeit bietet es die Verwaltung von lokalen „Zeitnormalen“, wie Funkuhren, an.

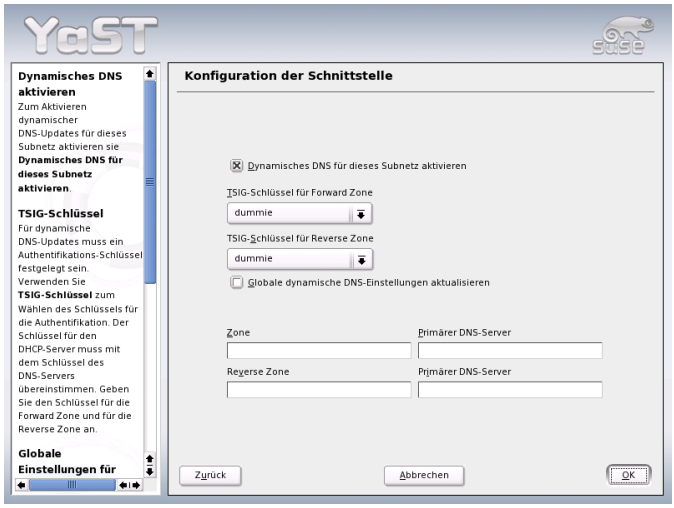

Abbildung 21.50: *DHCP-Server: Konfiguration der Schnittstelle für dynamisches DNS*

21.12.1 Konfiguration im Netzwerk

xntp ist so voreingestellt, dass nur die lokale Rechneruhr als Zeitreferenz dient. Die einfachste Möglichkeit, einen Zeitserver im Netz zu verwenden, ist die Angabe von „server“-Parametern. Steht im Netzwerk ein Zeitserver zur Verfügung, der zum Beispiel den Namen `ntp.example.com` hat, so können Sie diesen Server in der Datei `/etc/ntp.conf` folgendermaßen ergänzen: `server ntp.example.com`.

Weitere Zeitserver fügt man hinzu, indem man weitere Zeilen mit den Schlüsselwort „server“ einträgt. Nachdem der xntpd mit dem dem Befehl `rcxntpd start` initialisiert wurde, benötigt er eine Stunde, bis sich die Zeit stabilisiert hat und die „drift“-Datei zur Korrektur der lokalen Rechneruhr angelegt wird. Die drift-Datei hat langfristig den Vorteil, dass bereits nach dem Einschalten des Rechners bekannt ist, wie sich die Hardwareuhr im laufe der Zeit verstellt. Die Korrektur wird dann sofort aktiv, wodurch eine hohe Stabilität der Rechnerzeit erreicht wird.

Sofern in Ihrem Netzwerk der Zeitserver auch über einen Broadcast erreichbar ist, benötigen Sie den Server-Namen nicht. Tragen Sie in diesem Fall den Befehl `broadcastclient` in die Konfigurationsdatei `/etc/ntp.`

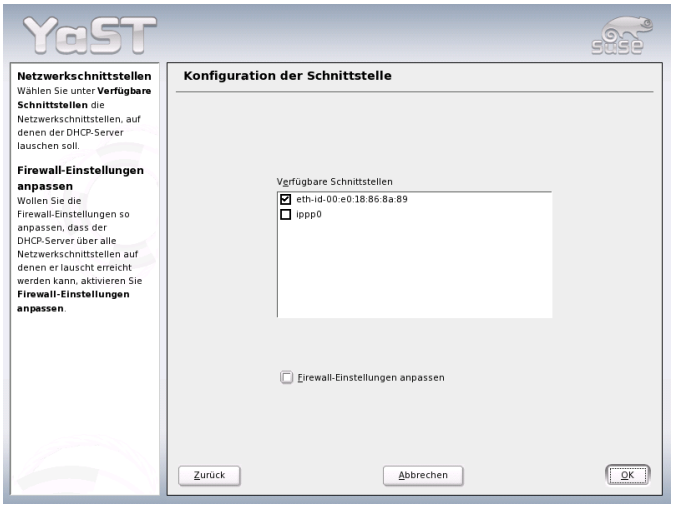

Abbildung 21.51: *DHCP-Server: Netzwerkschnittstelle und Firewall*

`conf` ein. In diesem Fall sollten Sie jedoch die Authentifizierungsmechanismen einrichten, da sonst ein fehlerhafter Zeitserver im Netzwerk die Rechnerzeit verändern würde.

Jeder xntpd kann im Netzwerk normalerweise auch als Zeitserver angesprochen werden. Wenn Sie den xntpd auch mit Broadcasts betreiben möchten, können Sie dies mit der Option `broadcast` einrichten:

```
broadcast 192.168.0.255
```

Ändern Sie hierzu die Broadcast-Adresse auf Ihre Gegebenheiten ab. Hierbei sollten Sie sicherstellen, dass der Zeitserver wirklich die richtige Uhrzeit verwendet. Hierzu eigenen sich zum Beispiel „Zeitnormalen“.

21.12.2 Einrichten einer lokalen Zeitnormalen

Das Programmpaket xntp enthält auch Treiber, die den Anschluss von lokalen Zeitnormalen erlauben. Die unterstützten Uhren finden Sie im Paket xntp-doc in der Datei `file:/usr/share/doc/packages/xntp-doc/html/refclock.htm`. Jedem Treiber ist hierbei eine Nummer zugeordnet. Die eigentliche Konfiguration geschieht bei xntp über sogenannte

Pseudo-IPs. Die Uhren werden in die Datei `/etc/ntp.conf` so eingetragen, als wären sie im Netzwerk verfügbare Uhren.

Hierzu bekommen sie spezielle IP-Adressen, die alle folgende Form haben: `127.127.`⟨*t*⟩`.`⟨*u*⟩. Den Wert von ⟨*t*⟩ bekommen Sie aus der oben genannten Datei mit der Liste der Referenzuhren. ⟨*u*⟩ ist die Gerätenummer, die nur dann von `0` abweicht, wenn Sie mehrere Uhren des gleichen Typs an dem Rechner verwenden. Eine „Type 8 Generic Reference Driver (PARSE)“ hat demnach die Pseudo-IP-Adresse `127.127.8.0`.

Die einzelnen Treiber haben im Normalfall spezielle Parameter, die die Konfiguration näher beschreiben. In der Datei `file:/usr/share/doc/packages/xntp-doc/html/refclock.htm` finden Sie zu jedem Treiber einen Link zur jeweiligen Treiberseite, die diese Parameter beschreiben. Für die Uhr mit dem „Typ 8“ ist es zum Beispiel notwendig, einen zusätzlichen mode anzugeben, der die Uhr genauer spezifiziert. So hat das Modul „Conrad DCF77 receiver module“ den „mode 5“. Damit diese Uhr von xntp als Referenz genommen wird, können Sie zusätzlich das Schlüsselwort `prefer` angeben. Die vollständige `server`-Zeile eines „Conrad DCF77 receiver module“ lautet somit:

```
server 127.127.8.0 mode 5 prefer
```

Andere Uhren folgen dem gleichen Schema. Die Dokumentation zu xntp steht nach der Installation des Pakets `xntp-doc` im Verzeichnis `/usr/share/doc/packages/xntp-doc/html` zur Verfügung.

Der Webserver Apache

Mit einem Anteil von über 60 Prozent (laut `http://www.netcraft.com`) ist Apache der weltweit am weitesten verbreitete Webserver. Für Web-Anwendungen wird Apache häufig mit Linux, der Datenbank MySQL und den Programmiersprachen PHP und Perl kombiniert. Für diese Kombination hat sich die Abkürzung *LAMP* eingebürgert.

22.1 Grundlagen 582
22.2 HTTP-Server mit YaST einrichten 583
22.3 Apache Module 584
22.4 Neuerungen mit Apache 2 585
22.5 Threads 586
22.6 Installation 587
22.7 Konfiguration 589
22.8 Apache im Einsatz 594
22.9 Aktive Inhalte 595
22.10 Virtual Hosts 601
22.11 Sicherheit 605
22.12 Troubleshooting 606
22.13 Weitere Dokumentation 607

22.1 Grundlagen

22.1.1 Webserver

Ein Webserver liefert auf Anfrage eines Clients HTML-Seiten an diesen aus. Diese Seiten können in einem Verzeichnis auf dem Server abgelegt sein (sogenannte passive oder statische Seiten) oder als Antwort auf die Anfrage neu generiert werden (aktive Inhalte).

22.1.2 HTTP

Bei den Clients handelt es sich meist um Webbrowser wie Konqueror und Mozilla. Die Kommunikation zwischen Browser und Webserver findet über das *H*yper*T*ext *T*ransfer *P*rotocol (HTTP) statt. Die aktuelle Version HTTP 1.1 ist im RFC 2068 sowie im Update RFC 2616 dokumentiert, diese RFCs findet man unter der URL `http://www.w3.org`.

22.1.3 URLs

Ein Client fordert über eine URL eine Seite vom Server an, zum Beispiel `http://www.suse.de/index.html` Eine URL besteht aus:

- Einem Protokoll. Häufig benutzte Protokolle sind
  - `http://` Das HTTP-Protokoll.
  - `https://` Sichere, verschlüsselte Version von HTTP.
  - `ftp://` *F*ile *T*ransfer *P*rotocol, zum Down- und Upload von Dateien.
- Einer Domain, in diesem Fall `www.suse.de`. Die Domain kann man nochmals unterteilen, der erste Teil `www` verweist auf einen Computer, der zweite Teil `suse.de` ist die eigentliche Domain. Beides zusammen wird auch als FQDN (Fully Qualified Domain Name) bezeichnet.
- Einer Resource, in diesem Fall `index.html`. Dieser Teil gibt den kompletten Pfad zur Resource an. Die Resource kann eine Datei sein, wie in diesem Fall. Es kann sich aber auch um ein CGI-Skript, eine Java Server Page etc. handeln.

Dabei wird die Weiterleitung der Anfrage an die Domain `www.suse.de` von den entsprechenden Mechanismen des Internet (zum Beispiel Domain Name System, DNS) übernommen, die den Zugriff auf eine Domain an einen oder mehrere dafür zuständige Rechner weiterleiten. Apache selbst liefert dann die Resource, in diesem Fall also einfach die Seite `index.html` aus seinem Dateiverzeichnis aus. In diesem Fall liegt die Datei auf der obersten Ebene des Verzeichnisses, sie kann aber auch in einem Unterverzeichnis liegen, zum Beispiel `http://www.suse.de/business/services/support/index.html`.

Der Pfad der Datei ist dabei relativ zur sogenannten DocumentRoot, diese kann in den Konfigurationsdateien geändert werden. Wie das geht, beschreibt der Abschnitt 22.7.2 auf Seite 590.

22.1.4 Automatische Ausgabe einer Standardseite

Die Angabe der Seite kann fehlen. Apache hängt dann automatisch einen der gebräuchlichen Namen für solche Seiten an die URL an. Der gebräuchlichste Name für eine solche Seite ist `index.html`. Ob Apache diesen Automatismus ausführt und welche Seitennamen dabei berücksichtigt werden, lässt sich einstellen, dies ist im Abschnitt 22.7.2 auf Seite 591 beschrieben. In diesem Fall reicht dann beispielsweise der Aufruf von `http://www.suse.de` um vom Server die Seite `http://www.suse.de/index.html` angezeigt zu bekommen.

22.2 HTTP-Server mit YaST einrichten

Apache 2 läßt sich einfach und schnell mit YaST einrichten. Allerdings sollten Sie über einige Kenntnisse verfügen, wenn Sie damit einen Webserver aufsetzen möchten. Wenn Sie im YaST-Kontrollzentrum auf 'Netzwerkdienste' -> 'HTTP-Server' klicken, werden Sie gegebenenfalls gefragt, ob YaST fehlende Pakete installieren soll. Ist alles installiert, gelangen Sie in den Konfigurationsdialog.

Aktivieren Sie hier zunächst den HTTP-Dienst. Standardmäßig sind drei Optionen vorgegeben: 'Servername', 'E-Mail des Serveradministrators' und 'Lauschen auf'. Bei letztere Option ist bereits Port 80 voreingestellt. Über die Schaltfläche 'Hinzufügen' wählen Sie weitere Optionen aus. Mit 'Bearbeiten' ändern Sie den Wert der selektierten Option, 'Löschen' entfernt die Option.

Über die Kombo-Box 'Erweitert' können Sie sich das 'Zugriffsprotokoll anzeigen', 'Fehlerprotokoll anzeigen' lassen und die vom Server zu ladenden 'Servermodule' konfigurieren. In dieser Maske aktivieren und deaktivieren Sie Module über die Schaltfläche 'Status wechseln' und nehmen zusätzliche Module über die Schaltfläche 'Modul hinzufügen' auf.

22.3 Apache Module

Apache kann über Module um viele Funktionen erweitert werden und dadurch mit Hilfe von Modulen CGI-Skripte in verschiedenensten Programmiersprachen ausführen. Hier stehen nicht nur Perl und PHP zur Verfügung, sondern auch weitere Skriptsprachen wie Python oder Ruby. Zudem gibt es Module für die gesicherte übertragung von Daten mit SSL (Secure Sockets Layer), die Authentifizierung von Benutzern, erweitertes Logging und vieles mehr ermöglichen.

Apache kann über selbstgeschriebene Module an alle ausgefallenen Anforderungen und Wünsche angepasst werden. Natürlich ist dazu ein gewisses Maß an Know-How nötig. Referenzen auf weiterführende Informationen finden Sie im Abschnitt 22.13.4 auf Seite 608

Wenn Apache eine Anfrage bearbeitet, können für die Bearbeitung dieser Anfrage einer oder mehrere Handler eingetragen sein. Dies geschieht über Anweisungen in der Konfigurationsdatei. Die Handler können Teil von Apache sein, es kann aber auch ein Modul für die Bearbeitung aufgerufen werden. Dadurch lässt sich dieser Vorgang sehr flexibel gestalten. Zudem besteht die Möglichkeit, eigene Module in Apache einzuklinken und so Einfluss auf die Bearbeitung der Anfragen zu nehmen.

Bei Apache 2 geht die Modularisierung recht weit, hier erfüllt der Server nur minimale Aufgaben, alles andere wird über Module realisiert. Das geht so weit, das bei Apache 2 selbst die Bearbeitung von HTTP über Module realisiert ist. Apache 2 muss demnach nicht unbedingt ein Webserver sein, er kann über andere Module auch ganz andere Aufgaben übernehmen. So gibt es als Modul beispielsweise einen Proof-of-Concept Mailserver (POP3) auf Apache-Basis.

Apache unterstützt eine Reihe von nützlichen Features, die im folgenden beschrieben werden.

Virtuelle Hosts Über virtuelle Hosts können mit einer Instanz von Apache auf einem einzigen Rechner mehrere Webseiten betrieben werden, wobei der Webserver für den Endbenutzer wie mehrere unab-

hängige Webserver wirkt. Dabei können die virtuellen Hosts auf unterschiedlichen IP-Addressen oder namensbasiert konfiguriert sein. Dies erspart die Anschaffungskosten und den Administrationsaufwand für zusätzliche Rechner.

Flexibles Umschreiben von URLs Apache bietet eine Vielzahl von Möglichkeiten, URLs zu manipulieren und umzuschreiben (URL-Rewriting). Näheres dazu findet man in der Dokumentation zu Apache.

Content Negotiation Apache kann in Abhängigkeit von den Fähigkeiten des Client (Browser) eine für diesen Client maßgeschneiderte Seite ausliefern. So kann man für ältere Browser oder Browser, die nur im Textmodus arbeiten (wie Lynx), einfachere Versionen der Seiten ausliefern, die keine Frames verwenden. Auf diese Weise kann man auch die notorischen Inkompatibilitäten der verschiedenen Browser, was JavaScript angeht, umgehen, indem man jedem Browser eine passende Version der Seiten liefert (wenn man den Aufwand treiben will, für jeden dieser Browser den JavaScript-Code anzupassen).

Flexible Fehlerbehandlung Falls ein Fehler auftritt, beispielsweise eine Seite nicht verfügbar ist, kann man flexibel reagieren und eine angemessene Antwort zurückgeben. Diese kann auch aktiv zusammengesetzt sein, beispielsweise mit Hilfe von CGI.

22.4 Neuerungen mit Apache 2

Im Folgenden finden Sie eine Liste der Neuerungen mit Apache 2. Ausführliche Dokumentation zum Apache HTTP Server Version 2.0 finden Sie auf der Webseite: `http://httpd.apache.org/docs-2.0/de/`.

- Bei der Art und Weise, wie mehrere Anfragen gleichzeitig ausgeführt werden, hat man die Wahl zwischen Threads und Prozessen. Die Prozessverwaltung ist in ein eigenes Modul, das sogenannte Multi-Processing-Modul (MPM) ausgelagert worden. Je nach MPM reagiert Apache 2 verschieden auf Anfragen. Das hat vor allem Auswirkungen auf die Performance und auf die Verwendung von Modulen. Dies wird im Folgenden ausführlicher besprochen.
- Das Innenleben von Apache wurde gründlich aufgeräumt, Apache verwendet nun eine neue, eigene Basisbibliothek (Apache Portable Runtime, APR) als Schnittstelle zu Systemfunktionen und für die

Speicherverwaltung. Darüberhinaus sind wichtige und weitverbreitete Module wie mod_gzip (Nachfolger: mod_deflate) oder mod_ssl, die tief in die Request-Verarbeitung eingreifen, jetzt weit besser in den Apache integriert.

- Apache 2 beherrscht nun das kommende Internetprotokoll IPv6.
- Es gibt jetzt einen Mechanismus, mit dem die Hersteller von Modulen selbst Angaben über die gewünschte Ladereihenfolge der Module machen können, so dass sich der Anwender nicht mehr selbst darum kümmern muss. Die Reihenfolge, in der Module ausgeführt werden, ist oft wichtig und wurde früher ueber die Ladereihenfolge festgelegt. So muss ein Modul, das nur authentifizierten Benutzern Zugriff auf bestimmte Resourcen erlaubt, als erstes aufgerufen werden, damit Benutzer, die keine Zugriffsrechte haben, die Seiten erst gar nicht zu sehen bekommen können.
- Anfragen an und Antworten von Apache können durch Filter bearbeitet werden.
- Unterstützung fuer Dateien größer 2 GiB (Large-File-Support, LFS), auf 32-bit-Systemen
- Einige neuere Module gibt es nur für Apache 2.
- Mehrsprachige Fehlermeldungen.

22.5 Threads

Ein Thread ist eine Art leichtgewichtiger Prozess, der im Vergleich zu einem richtigen Prozess wesentlich weniger Ressourcen verbraucht. Dadurch steigt bei der Verwendung von Threads statt Prozessen auch die Performance. Der Nachteil ist dabei, dass Anwendungen für die Ausführung in einer Thread-Umgebung thread-safe sein müssen. Dies bedeutet:

- Funktionen (bzw. bei objektorientierten Anwendungen die Methoden) müssen „reentrant“ sein, das heißt dass die Funktion mit dem gleichen Input immer das gleiche Ergebnis liefert, unabhängig davon ob sie gleichzeitig von anderen Threads ausgeführt wird. Funktionen müssen demnach so programmiert sein, dass sie von mehreren Threads gleichzeitig aufgerufen werden können.

- Der Zugriff auf Resourcen (meistens Variablen) muss so geregelt sein, dass sich die gleichzeitig laufenden Threads dabei nicht in die Quere kommen.

Apache 2 kann Anfragen als eigene Prozesse oder in einem gemischten Modell mit Prozessen und Threads ausführen. Für die Ausführung als Prozess sorgt das MPM „prefork“, für die Ausführung als Thread das MPM „worker“. Bei der Installation (siehe Abschnitt 22.6) kann man auswählen, welches MPM verwendet werden soll. Der dritte Modus, „perchild“ ist noch nicht voll ausgereift und steht deswegen in SUSE LINUX bei der Installation (noch) nicht zur Verfügung.

22.6 Installation

22.6.1 Paketauswahl in YaST

Für einfache Anforderungen muss man lediglich das Apache-Paket `apache2` installieren. Installieren Sie zusätzlich eines der MPM-Pakete (Multiprocessing Module) wie das Paket `apache2-prefork` oder `apache2-worker`. Bei der Auswahl des richtigen MPM ist zu beachten, dass das mit Threads laufende Worker-MPM nicht mit Paket `mod_php4` zusammen verwendet werden kann, da noch nicht alle von diesem Paket verwendeten Bibliotheken threadsafe sind.

22.6.2 Apache aktivieren

Wenn Apache installiert ist, wird er nicht automatisch gestartet. Um Apache zu starten, muss man ihn im Runlevel-Editor aktivieren. Um ihn dauerhaft beim Booten des Systems zu starten, muss man im Runlevel-Editor für die Runlevel 3 und 5 ein Häkchen setzen. Ob Apache läuft, lässt sich feststellen, indem man die URL `http://localhost/` in einem Browser aufruft. Läuft Apache, kann dann eine Beispielseite sehen, sofern das Paket `apache2-example-pages` installiert ist.

22.6.3 Module für aktive Inhalte

Um aktive Inhalte mit Hilfe von Modulen zu nutzen, muss man noch die Module für die jeweiligen Programmiersprachen installieren. Dies sind das Paket `apache2-mod_perl` für Perl bzw. das Paket `apache2-mod_php4`

für PHP und schließlich das Paket `apache2-mod_python` für Python. Die Verwendung dieser Module ist im Abschnitt 22.9.5 auf Seite 598 beschrieben.

22.6.4 Zusätzliche empfehlenswerte Pakete

Zusätzlich empfiehlt es sich, die reichhaltige Dokumentation zu installieren, diese findet sich im Paket `apache2-doc`. Für diese Dokumentation existiert ein Alias (was das ist, wird im Abschnitt 22.7 auf der nächsten Seite beschrieben), so dass man sie nach der Installation direkt über die URL `http://localhost/manual` aufrufen kann.

Wer Module für Apache entwickeln oder Module von Drittanbietern kompilieren will, muss noch das Paket `apache2-devel` installieren, sowie entsprechende Entwicklungswerkzeuge. Diese enthalten unter anderem die `apxs`-Tools, die im Abschnitt 22.6.5 näher beschrieben sind.

22.6.5 Installation von Modulen mit apxs

Ein wichtiges Werkzeug für Modulentwickler ist apxs2. Mit diesem Programm lassen sich Module , die als Quelltext vorliegen, mit einem einzigen Befehl kompilieren und installieren, samt der notwendigen Änderungen an den Konfigurationsdateien. Außerdem kann man auch Module installieren, die bereits als Objektdatei (Endung `.o`) oder statische Library (Endung `.a`) vorliegen. apxs2 erstellt aus den Quellen ein Dynamic Shared Object (DSO), das von Apache direkt als Modul verwendet wird.

Die Installation eines Moduls aus dem Quelltext bewirkt beispielsweise der Befehl `apxs2 -c -i -a mod_foo.c`. Andere Optionen von `apxs2` sind in der zugehörigen Manpage beschrieben.

Von apxs2 gibt es mehrere Versionen: `apxs2`, `apxs2-prefork` und `apxs2-worker`. Während `apxs2` ein Modul so installiert, dass es für alle MPMs verwendbar ist, installieren die beiden anderen Programme Module so, dass sie nur für die jeweiligen MPMs (also prefork bzw. worker) verwendet werden. Während also `apxs2` ein Modul in `/usr/lib/apache2/` installiert, landet dieses Modul bei Verwendung von `apxs2-prefork` in `/usr/lib/apache2-prefork/`.

Die Option `-a` sollte mit Apache 2 nicht verwendet werden, da dann die Änderungen direkt in `/etc/apache2/httpd.conf/` geschrieben werden. Stattdessen sollten Module über den Eintrag `APACHE_MODULES` in `/etc/sysconfig/apache2/` aktiviert werden, wie im Abschnitt 22.7.1 auf der nächsten Seite beschrieben.

22.7 Konfiguration

Wenn man Apache installiert hat, sind weitere Anpassungen nur nötig, wenn man spezielle Wünsche oder Anforderungen hat. Apache kann einerseits über SuSEconfig konfiguriert werden, andererseits kann man auch die Datei `/etc/apache2/httpd.conf/` direkt editieren.

22.7.1 Konfiguration mit SuSEconfig

Die Einstellungen, die Sie in `/etc/sysconfig/apache2` vornehmen können, werden mittels SuSEconfig in die Konfigurationsdateien von Apache eingepflegt. Diese umfassen jene Konfigurationsmöglichkeiten, die für viele Fälle ausreichend sein dürften. Zu jeder Variable finden Sie erläuternde Kommentare in der Datei.

Eigene Konfigurationsdateien

Statt Änderungen in der Konfigurationsdatei `/etc/apache2/httpd.conf` direkt vorzunehmen, kann man mit Hilfe der Variablen `APACHE_CONF_INCLUDE_FILES` eine eigene Konfigurationsdatei angeben (beispielsweise `httpd.conf.local`), die dann in die Hauptkonfigurationsdatei eingelesen wird. Auf diese Weise bleiben auch eigene Änderungen an der Konfiguration erhalten, wenn die Datei `/etc/apache2/httpd.conf` bei einer Neuinstallation überschrieben wird.

Module

Module, die per YaST bereits installiert wurden, werden aktiviert, indem man den Namen des Moduls in die für die Variable `APACHE_MODULES` angegebene Liste aufnimmt. Diese Variable findet sich in der Datei `/etc/sysconfig/apache2`.

Flags

Mit der Variable `APACHE_SERVER_FLAGS` können Flags angegeben werden, die bestimmte Bereiche in der Konfigurationsdatei an- und ausschalten. Ist also in der Konfigurationsdatei ein Abschnitt in

```
<IfDefine someflag>
.
.
.
</IfDefine>
```

eingeschlossen, so wird dieser nur aktiviert, wenn bei in der Variable `ACTIVE_SERVER_FLAGS` das entsprechende Flag gesetzt ist: `ACTIVE_SERVER_FLAGS = ... someflag ...` Auf diese Weise können größere Bereiche der Konfigurationsdatei zu Testzwecken einfach aktiviert oder deaktiviert werden.

22.7.2 Manuelle Konfiguration

Die Konfigurationsdatei

Die Konfigurationsdatei `/etc/apache2/httpd.conf` erlaubt Änderungen, die über Einstellungen in `/etc/sysconfig/apache2` nicht möglich sind. Es folgen einige der Parameter, die dort eingestellt werden können. Sie sind ungefähr in der Reihenfolge aufgelistet, in der sie in dieser Datei vorkommen.

DocumentRoot

Eine grundlegende Einstellung ist die sogenannte `DocumentRoot`, das ist das Verzeichnis, unter dem Apache Webseiten erwartet, die vom Server ausgeliefert werden sollen. Sie ist für den Default-Virtual Host auf `/srv/www/htdocs` eingestellt und muss normalerweise nicht geändert werden.

Timeout

Gibt die Zeit an, die der Server wartet, bis er einen Timeout für eine Anfrage meldet.

MaxClients

Die Anzahl der Clients, die Apache maximal gleichzeitig bedient. Die Voreinstellung ist `150`, dieser Wert könnte für eine viel besuchte Website aber auch zu niedrig sein.

LoadModule

Die `LoadModule` Anweisungen geben an, welche Module geladen werden. In Apache 2 wird die Ladereihenfolge durch die Module selbst angegeben, siehe dazu auch den Abschnitt 22.4 auf Seite 585. Ausserdem geben diese Anweisungen an, welche Datei das Modul enthält.

Port

Gibt den Port an, auf dem Apache auf Anfragen wartet. Dies ist normalerweise immer Port 80, der Standardport für HTTP. Diese Einstellung zu ändern, ist im Normalfall nicht sinnvoll. Ein Grund, Apache auf einem anderen Port lauschen zu lassen, kann der Test einer neuen Version einer Website sein. Auf diese Weise ist die funktionierende Version der Website nach wie vor über den Standardport 80 erreichbar.

Ein weiterer Grund kann sein, dass man Seiten lediglich im Intranet zur Verfügung stellen will, weil sie Informationen enthalten, die nicht jeden etwas angehen. Dazu stellt man den Port beispielsweise auf den Wert 8080 ein und sperrt Zugriffe von aussen auf diesen Port in der Firewall. So ist der Server vor jedem Zugriff von ausserhalb abgesichert.

Directory

Mit dieser Direktive werden die Zugriffs- und andere Rechte für ein Verzeichnis gesetzt. Auch für die `DocumentRoot` existiert eine solche Direktive, der dort angegebene Verzeichnisnname muss immer parallel mit `DocumentRoot` geändert werden.

DirectoryIndex

Hiermit kann eingestellt werden, nach welchen Dateien Apache sucht, um eine URL zu vervollständigen, bei der die Angabe der Datei fehlt. Die Voreinstellung ist `index.html`. Wird also beispielsweise vom Client die URL `http://www.xyz.com/foo/bar` aufgerufen und existiert unterhalb der DocumentRoot ein Verzeichnis `foo/bar`, das eine Datei names `index.html` enthält, so liefert Apache diese Seite an den Client zurück.

AllowOverride

Jedes Verzeichnis, aus dem Apache Dokumente ausliefert, kann eine Datei enthalten, die global eingestellte Zugriffsrechte und andere Einstellungen für dieses Verzeichnis abändern kann. Diese Einstellungen gelten rekursiv für das aktuelle Verzeichnis und seine Unterverzeichnisse, bis sie in einem Unterverzeichnis von einer weiteren solchen Datei geändert werden. Dies bedeutet auch, dass solche Einstellungen, wenn sie in einer Datei in `DocumentRoot` angegeben sind, global gelten. Diese Dateien haben normalerweise den Namen `.htaccess`, man kann das jedoch ändern, siehe dazu den Abschnitt 22.7.2 auf der nächsten Seite.

Mit `AllowOverride` kann man einstellen, ob die in den lokalen Dateien angegebenen Einstellungen die globalen Einstellungen überschreiben können. Mögliche Werte sind `None`, `All` sowie jede mögliche Kombination von `Options`, `FileInfo`, `AuthConfig` und `Limit`. Die Bedeutung dieser Werte ist in der Dokumentation zu Apache ausführlich beschrieben. Die (sichere) Voreinstellung ist `None`.

Order

Diese Option beeinflusst, in welcher Reihenfolge die Einstellungen für die Zugriffsrechte `Allow`, `Deny` angewandt werden. Die Voreinstellung ist:

```
Order allow,deny
```

Es werden also zuerst die Zugriffsrechte für erlaubte Zugriffe und dann die für verbotene Zugriffe angewandt. Die zugrundeliegende Denkweise ist eine von zweien:

allow all jeden Zugriff erlauben, aber Ausnahmen definieren.

deny all jeden Zugriff verweigern, aber Ausnahmen definieren.

Beispiel für `deny all`:

```
Order deny,allow
Deny from all
Allow from example.com
Allow from 10.1.0.0/255.255.0.0
```

AccessFileName

Hier lässt sich der Name für die Dateien einstellen, die in von Apache ausgelieferten Verzeichnissen die globalen Einstellungen für Zugriffsrechte etc. überschreiben können (siehe dazu auch Abschnitt 22.7.2 auf der vorherigen Seite). Die Voreinstellung ist `.htaccess`.

ErrorLog

Gibt den Namen der Datei an, in der Apache Fehlermeldungen ausgibt. Die Voreinstellung ist `/var/log/httpd/errorlog`. Fehlermeldungen für Virtual Hosts (siehe Abschnitt 22.10 auf Seite 601) werden ebenfalls in diese Datei ausgegeben, wenn im `VirtualHost-Abschnitt` der Konfigurationsdatei keine eigene Log-Datei angegeben wurde.

LogLevel

Fehlermeldungen werden je nach Dringlichkeit in verschiedene Stufen eingeteilt. Diese Einstellung gibt an, ab welcher Dringlichkeitsstufe die Meldungen ausgeben werden. Eine Einstellung auf einen Level gibt an, dass Meldungen dieser Stufe und dringendere Meldungen ausgegeben werden. Voreinstellung ist `warn`.

Alias

Mit einem Alias kann man einen Shortcut für ein Verzeichnis angeben, mit dem man dann direkt auf dieses Verzeichnis zugreifen kann. So kann man beispielsweise über das Alias `/manual/` auf das Verzeichnis `/srv/www/htdocs/manual` zugreifen, auch wenn die DocumentRoot auf ein anderes Verzeichnis als `/srv/www/htdocs` eingestellt ist. Solange die DocumentRoot diesen Wert hat, macht das keinen Unterschied. Im Falle dieses Alias kann man dann direkt mit `http://localhost/manual` auf das entsprechende Verzeichnis zugreifen. Eventuell kann es nötig sein, für das in einer `Alias`-Direktive angegebene Zielverzeichnis eine`Directory`-Direktive anzugeben, in der die Rechte für das Verzeichnis eingestellt werden (vgl. Abschnitt 22.7.2 auf Seite 591).

ScriptAlias

Diese Anweisung ähnelt der Alias-Anweisung. Sie gibt zusätzlich an, dass die Dateien im Zielverzeichnis als CGI-Skripte behandelt werden sollen.

Server Side Includes

Server Side Includes können aktiviert werden, indem man alle ausführbaren Dateien nach SSIs durchsuchen lässt. Dies geschieht mit der folgenden Anweisung:

```
<IfModule mod_include.c>
XBitHack on
</IfModule>
```

Um eine Datei nach Server Side Includes durchsuchen zu lassen, muss man sie dann lediglich mit `chmod +x` ⟨*dateiname*⟩ ausführbar machen. Alternativ kann man auch explizit den Typ der Dateien angeben, die nach SSIs durchsucht werden sollen. Dies geschieht mit

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Es ist keine gute Idee, hier einfach `.html` anzugeben, da Apache dann alle Seiten nach Server Side Includes durchsucht (auch solche, die mit Sicherheit keine solchen enthalten), was die Performance erheblich beeinträchtigt. Bei SUSE LINUX sind diese beiden Anweisungen bereits in der Konfigurationsdatei eingetragen, es sind also normalerweise keine Anpassungen nötig.

UserDir

Mit Hilfe des Moduls `mod_userdir` und der Direktive `UserDir` kann man ein Verzeichnis im Home-Verzeichnis des Anwenders angeben, in dem dieser seine Dateien über Apache veröffentlichen kann. Dies wird in SuSEconfig über die Variable `HTTPD_SEC_PUBLIC_HTML` eingestellt. Um Dateien veröffentlichen zu können, muss diese Variable auf den Wert `yes` gesetzt sein. Dies führt zu folgendem Eintrag in der Datei `/etc/httpd/suse_public_html.conf`, die von `/etc/apache2/httpd.conf` eingelesen wird.

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```

22.8 Apache im Einsatz

Um mit Apache eigene (statische) Webseiten anzuzeigen, muss man lediglich die eigenen Dateien im richtigen Verzeichnis unterbringen. Unter SUSE LINUX ist das `/srv/www/htdocs`. Eventuell sind dort bereits ein paar kleine Beispielseiten installiert. Diese dienen lediglich dazu, nach der Installation zu testen, ob Apache korrekt installiert wurde und läuft, man kann sie problemlos überschreiben oder besser deinstallieren. Eigene CGI-Skripte werden unter `/srv/www/cgi-bin` installiert.

Apache schreibt im laufenden Betrieb Log-Meldungen in die Datei `/var/log/httpd/access_log` bzw. `/var/log/apache2/access_log`. Dort ist dokumentiert, welche Ressourcen zu welcher Zeit mit welcher Methode (`GET`, `POST` ...) angefragt und ausgeliefert wurden. Bei Fehlern finden sich entsprechende Hinweise unter `/var/log/apache2`).

22.9 Aktive Inhalte

Apache bietet mehrere Möglichkeiten, aktive Inhalte an Clients auszuliefern. Unter aktiven Inhalten versteht man HTML-Seiten, die aufgrund einer Verarbeitung aus variablen Eingabedaten des Clients erstellt wurden. Ein bekanntes Beispiel dafür sind Suchmaschinen, die auf die Eingabe eines oder mehrerer, eventuell durch logische Operatoren wie UND bzw. ODER verknüpfter Suchbegriffe eine Liste von Seiten zurückgeben, in denen diese Begriffe vorkommen.

Mit Apache gibt es drei Wege, um aktive Inhalte zu erstellen:

Server Side Includes (SSI) Dabei handelt es sich um Anweisungen, die mit Hilfe spezieller Kommentare in eine HTML-Seite eingebettet werden. Apache wertet den Inhalt der Kommentare aus und gibt das Ergebnis als Teil der HTML-Seite mit aus.

Common Gateway Interface (CGI)
Hierbei werden Programme ausgeführt, die innerhalb bestimmter Verzeichnisse liegen. Apache übergibt vom Client übertragene Parameter an diese Programme und gibt die Ausgabe des Programms an den Client zurück. Diese Art der Programmierung ist relativ einfach, zumal man existierende Kommandozeilenprogramme so umbauen kann, dass sie Eingaben von Apache annehmen und Ausgaben an ihn ausgeben.

Module Apache bietet Schnittstellen, um beliebige Module als Teil der Verarbeitung einer Anfrage ausführen zu können, und gewährt diesen Programmen zudem Zugriff auf wichtige Informationen, wie den Request oder die HTTP-Header. Dies macht es möglich, Programme in die Verarbeitung der Anfrage einzufügen, die nicht nur aktive Inhalte erzeugen können, sondern auch andere Funktionen (wie Authentifizierung) übernehmen können. Die Programmierung solcher Module erfordert etwas Geschick, als Vorteil wiegt eine hohe Performance sowie Möglichkeiten, die sowohl über SSI als auch über CGI weit hinausgehen.

Während CGI-Skripte einfach von Apache aufgerufen werden (unter der Benutzer-ID ihres Eigentümers), wird bei Verwendung von Modulen ein Interpreter in Apache eingebettet, der dann unter der ID des Webservers permanent läuft. Der Interpreter ist „persistent“. Auf diese Weise muss nicht für jede Anfrage ein eigener Prozess gestartet und beendet werden

(was einen erheblichen Overhead für Prozessmanagement, Speicherverwaltung usw. nach sich zieht), stattdessen wird das Skript einfach an den bereits laufenden Interpreter übergeben.

Einen Nachteil hat die Sache allerdings: Während über CGI ausgeführte Skripte einigermaßen tolerant gegen nachlässige Programmierung sind, wirkt sich diese bei Verwendung von Modulen schnell nachteilig aus. Der Grund dafür ist, dass bei normalen CGI-Skripten Fehler wie das Nichtfreigeben von Resourcen und Speicher nicht so sehr ins Gewicht fallen, da die Programme nach Bearbeitung der Anfrage wieder beendet werden und damit vom Programm aufgrund eines Programmierfehlers nicht freigegebener Speicher wieder verfügbar wird. Bei Verwendung von Modulen häufen sich die Auswirkungen von Programmierfehlern an, da der Interpreter permanent läuft. Wenn der Server nicht neu gestartet wird, kann der Interpreter ohne weiteres monatelang laufen, da machen sich nicht freigegebene Datenbankverbindungen oder ähnliches durchaus bemerkbar.

22.9.1 Server Side Includes: SSI

Server Side Includes sind in spezielle Kommentare eingebettete Anweisungen, die Apache ausführt. Das Ergebnis wird dann an Ort und Stelle in die Ausgabe eingebettet. Ein Beispiel: Das aktuelle Datum kann man mit `<!--#echo var="DATE_LOCAL" -->` ausgegeben werden. Hierbei ist das # dem Kommentaranfang `<!--` der Hinweis für Apache, dass es sich um eine SSI-Anweisung und nicht um einen gewöhnlichen Kommentar handelt.

SSIs können auf mehrere Arten aktiviert werden. Die einfache Variante ist, alle Dateien, deren Rechte auf ausführbar gesetzt sind, auf Server Side Includes zu untersuchen. Die andere Variante ist, für bestimmte Dateitypen festzulegen, dass sie auf SSIs untersucht werden sollen. Beide Einstellungen werden im Abschnitt 22.7.2 auf Seite 593 erläutert.

22.9.2 Common Gateway Interface: CGI

CGI ist eine Abkürzung für „Common Gateway Interface“. Mit CGI liefert der Server nicht einfach eine statische HTML-Seite aus, sondern führt ein Programm aus, das die Seite liefert. Auf diese Weise können Seiten erstellt werden, die das Ergebnis einer Berechnung sind, beispielsweise das Ergebnis einer Suche in einer Datenbank. An das ausgeführte Programm können Argumente übergeben werden, so kann es für jede Anfrage eine individuelle Antwort-Seite zurückliefern.

Der große Vorteil an CGI ist, dass es eine recht einfache Technik ist. Das Programm muss lediglich in einem bestimmten Verzeichnis liegen und wird dann vom Webserver genauso wie ein Programm auf der Kommandozeile ausgeführt. Die Ausgaben des Programms auf dem Standardausgabekanal (`stdout`) gibt der Server einfach an den Client aus.

22.9.3 GET und POST

Eingabeparameter können entweder mit `GET` oder mit `POST` an den Server übergeben werden. Je nachdem, welche Methode verwendet wird, gibt der Server die Parameter auf unterschiedliche Weise an das Skript weiter. Bei `POST` übergibt der Server die Parameter auf dem Standardeingabekanal (`stdin`) an das Programm. Genauso würde das Programm seinen Input erhalten, wenn es in einer Konsole gestartet wird.

Bei `GET` werden die Parameter vom Server in der Umgebungsvariablen `QUERY_STRING` an das Programm übergeben. Eine Umgebungsvariable ist eine Variable, die vom System überall verfügbar gemacht wird, ein klassisches Beispiel ist die Variable `PATH`, die eine Liste von Pfaden enthält, die das System nach ausführbaren Kommandos durchsucht, wenn der Anwender einen Befehl eingibt.

22.9.4 Sprachen für CGI

CGI-Programme können prinzipiell in jeder Programmiersprache geschrieben sein. Typischerweise werden Skriptprachen (interpretierte Sprachen) wie Perl oder PHP verwendet, für geschwindigkeitskritische CGIs kann im Einzelfall auch C oder C++ die erste Wahl sein.

Im einfachsten Fall erwartet Apache diese Programme in einem bestimmten Verzeichnis (`cgi-bin`). Dieses Verzeichnis lässt sich in der Konfigurationsdatei einstellen, siehe den Abschnitt 22.7 auf Seite 589.

Ausserdem lassen sich weitere Verzeichnisse freigeben, die Apache dann nach ausführbaren Programmen durchsucht. Dies stellt aber ein gewisses Sicherheitsrisiko dar, da dann jeder Anwender (evtl. böswillige) Programme von Apache ausführen lassen kann. Wenn man ausführbare Programme lediglich in `cgi-bin` zulässt, kann der Administrator leichter kontrollieren, wer welche Skripte und Programme dort ablegt und ob diese evtl. bösartiger Natur sind.

22.9.5 Aktive Inhalte mit Modulen erzeugen

Es gibt eine Reihe von Modulen für die Verwendung in Apache. Alle im Folgenden beschriebenen Module stehen als Pakete in SUSE LINUX zur Verfügung. Der Begriff Modul wird in zwei Bedeutungen verwendet. Zum einen gibt es Module, die in Apache eingebaut werden können und dort eine bestimmte Funktion übernehmen, wie zum Beispiel die im Folgenden vorgestellten Module zur Einbettung von Programmiersprachen in Apache.

Zum anderen spricht man in Programmiersprachen von Modulen, wenn man eine abgeschlossene Menge von Funktionen, Klassen und Variablen meint. Diese Module werden in ein Programm eingebunden, um eine bestimmte Funktionalität zur Verfügung zu stellen. Ein Beispiel sind die in allen Skriptsprachen vorhandenen CGI-Module, die das Programmieren von CGI-Anwendungen erleichtern, indem sie unter anderem Methoden zum Lesen der Request-Parameter und zur Ausgabe von HTML-Code zur Verfügung stellen.

22.9.6 mod_perl

Perl ist eine weitverbreitete und bewährte Skriptsprache. Für Perl gibt es eine riesige Menge an Modulen und Bibliotheken (unter anderem auch eine Bibliothek zur Erweiterung der Konfigurationsdatei von Apache). Die Homepage für Perl ist `http://www.perl.com/`. Eine grosse Auswahl an Libraries für Perl findet man im Comprehensive Perl Archive Network (CPAN): `http://www.cpan.org/`. Eine deutschsprachige Seite für Perl-Programmierer ist `http://www.perlunity.de/`.

mod_perl einrichten

Um `mod_perl` unter SUSE LINUX einzurichten, muss man lediglich das entsprechende Paket installieren (siehe dazu den Abschnitt 22.6 auf Seite 587). Die erforderlichen Einträge in der Konfigurationsdatei für Apache sind dann ebenfalls schon vorhanden, siehe `/etc/apache2/mod_perl-startup.pl`. Informationen über `mod_perl` finden sich vor allem hier: `http://perl.apache.org/`

mod_perl vs. CGI

Im einfachsten Fall kann man ein bisheriges CGI-Skript als `mod_perl`-Skript laufen lassen, indem man es unter einer anderen URL aufruft. Die

Konfigurationsdatei enthält Aliase, die auf das gleiche Verzeichnis verweisen und darin enthaltene Skripte entweder über CGI oder über `mod_perl` aufrufen. Alle diese Einträge sind in der Konfigurationsdatei bereits eingetragen. Der Alias-Eintrag für CGI lautet:

```
ScriptAlias /cgi-bin/ "/srv/www/cgi-bin/"
```

Die Einträge für `mod_perl` lauten wie folgt:

```
<IfModule mod_perl.c>
# Provide two aliases to the same cgi-bin directory,
# to see the effects of the 2 different mod_perl modes.
# for Apache::Registry Mode
ScriptAlias /perl/          "/srv/www/cgi-bin/"
# for Apache::Perlrun Mode
ScriptAlias /cgi-perl/      "/srv/www/cgi-bin/"
</IfModule>
```

Die folgenden Einträge sind für `mod_perl` ebenfalls nötig. Auch sie sind bereits in der Konfigurationsdatei eingetragen.

```
#
# If mod_perl is activated, load configuration information
#
<IfModule mod_perl.c>
Perlrequire /usr/include/apache/modules/perl/startup.perl
PerlModule Apache::Registry

#
# set Apache::Registry Mode for /perl Alias
#
<Location /perl>
SetHandler  perl-script
PerlHandler Apache::Registry
Options ExecCGI
PerlSendHeader On
</Location>

#
# set Apache::PerlRun Mode for /cgi-perl Alias
#
<Location /cgi-perl>
SetHandler  perl-script
PerlHandler Apache::PerlRun
```

```
Options ExecCGI
PerlSendHeader On
</Location>

</IfModule>
```

Diese Einträge legen Aliase für die Modi `Apache::Registry` und `Apache::PerlRun` an. Der Unterschied zwischen den beiden Modi gestaltet sich folgendermaßen:

Apache::Registry Alle Skripte werden kompiliert und dann in einem Cache gehalten. Jedes Skript wird als Inhalt einer Subroutine angelegt. Dies ist gut für die Performance, hat jedoch auch einen Nachteil: Die Skripte müssen sehr sauber programmiert sein, da Variablen und Subroutinen zwischen den Aufrufen erhalten bleiben. Das bedeutet, dass man Variablen selbst zurücksetzen muss, damit sie beim nächsten Aufruf erneut verwendet werden können. Speichert man beispielsweise in einem Skript für Online-Banking die Kreditkartennummer eines Kunden in einer Variable auf, so könnte diese Nummer wieder auftauchen, wenn der nächste Kunde die Anwendung benutzt und somit das gleiche Skript wieder aufruft.

Apache::PerlRun Die Skripte werden für jede Anfrage neu kompiliert, sodass Variablen und Subroutinen zwischen den Aufrufen aus dem Namespace verschwinden. Der Namespace ist die Gesamtheit aller Variablennamen und Routinennamen, die zu einem bestimmten Zeitpunkt während der Existenz eines Skripts definiert sind. Mit `Apache::PerlRun` muss man deswegen nicht so genau auf saubere Programmierung achten, da alle Variablen beim Start des Skripts frisch initialisiert sind und keine Werte aus vorangegangenen Aufrufen mehr enthalten können. Dies geht natürlich zu Lasten der Geschwindigkeit, ist aber immer noch deutlich schneller als CGI, da man sich den Aufruf eines eigenen Prozesses für den Interpreter spart. `Apache::PerlRun` verhält sich ähnlich wie CGI.

22.9.7 mod_php4

PHP ist eine Programmiersprache, die speziell für den Einsatz mit Webservern entworfen wurde. Im Unterschied zu anderen Sprachen, deren Befehle in eigenständigen Dateien (Skripten) abgelegt werden, sind bei PHP die Befehle (ähnlich wie bei SSI) in eine HTML-Seite eingebettet. Der PHP-Interpreter verarbeitet die PHP-Befehle und bettet das Ergebnis der Verarbeitung in die HTML-Seite ein.

Die Homepage für PHP findet man unter `http://www.php.net/`. Eine deutschsprachige PHP-Seite findet man unter `http://www.php-homepage.de/`.

Das Paket `mod_php4-core` muss in jedem Fall installiert sein. Für Apache 2 wird zusätzlich Paket `apache2-mod_php4`.

22.9.8 mod_python

Python ist eine objektorientierte Programmiersprache mit einer sehr klaren und leserlichen Syntax. Etwas ungewöhnlich, aber nach einer kurzen Eingewöhnungsphase recht angenehm ist, dass die Struktur des Programms von der Einrückung abhängt. Blocks werden nicht über geschweifte Klammern (wie in C und Perl) oder andere Begrenzer (wie `begin` und `end`) definiert, sondern darüber, wie tief sie eingerückt sind. Installieren Sie Paket `apache2-mod_python`.

Mehr über die Sprache findet man unter `http://www.python.org/`. Mehr Informationen über `mod_python` bietet `http://www.modpython.org/`.

22.9.9 mod_ruby

Ruby ist eine relativ junge objektorientierte High-Level-Programmiersprache, die sowohl Ähnlichkeit mit Perl als auch mit Python hat und die sich hervoragend für Skripte eignet. Mit Python verbindet sie die saubere, sehr übersichtliche Syntax, während sie von Perl die von vielen Programmierern geliebten (und von anderen verachteten) Kürzel wie zum Beispiel `$.r`, die Nummer der zuletzt aus der Eingabedatei gelesenen Zeile, übernommen hat. Von der grundlegenden Konzeption erinnert Ruby stark an Smalltalk.

Die Homepage von Ruby ist `http://www.ruby-lang.org/`. Auch für Ruby gibt es ein Apache-Modul, die Homepage findet sich unter `http://www.modruby.net/`.

22.10 Virtual Hosts

Mit Virtual Hosts ist es möglich, mehrere Domains mit einem einzigen Webserver ins Netz zu stellen. Auf diese Weise spart man sich die Kosten und den Administrationsaufwand für einen eigenen Server pro Domain.

Apache war einer der ersten Webserver, die dieses Feature geboten haben und er bietet mehrere Möglichkeiten für Virtual Hosts:

- Namensbasierte Virtual Hosts
- IP-basierte Virtual Hosts
- Mehrere Instanzen von Apache auf einem Rechner laufen lassen.

22.10.1 Namensbasierte Virtual Hosts

Bei namensbasierten Virtual Hosts werden von einer Instanz von Apache mehrere Domains bedient. Die Einrichtung mehrerer IPs für einen Rechner ist hierbei nicht nötig. Dies ist die einfachste Alternative und sie sollte bevorzugt werden. Mehr zu Gründen, die gegen die Verwendung von namensbasierten Virtual Hosts sprechen können, findet man in der Dokumentation zu Apache.

Diese Konfiguration geschieht direkt über die Konfigurationsdatei `/etc/apache2/httpd.conf`. Um namensbasierte Virtual Hosts zu aktivieren, muss man eine passende Direktive angeben: `NameVirtualHost *`. Hier reicht die Angabe von `*`, damit Apache einfach alle eingehenden Anfragen entgegen nimmt. Dann müssen noch die einzelnen Hosts konfiguriert werden:

```
<VirtualHost *>
    ServerName www.meinefirma.de
    DocumentRoot /srv/www/htdocs/meinefirma.de
    ServerAdmin webmaster@meinefirma.de
    ErrorLog /var/log/httpd/www.meinefirma.de-error_log
    CustomLog /var/log/httpd/www.meinefirma.de-access_log common
</VirtualHost>

<VirtualHost *>
    ServerName www.meineanderefirma.de
    DocumentRoot /srv/www/htdocs/meineanderefirma.de
    ServerAdmin webmaster@meineanderefirma.de
    ErrorLog /var/log/httpd/www.meineanderefirma.de-error_log
    CustomLog /var/log/httpd/www.meineanderefirma.de-access_log common
</VirtualHost>
```

Hier wie im Folgenden sollte für Apache 2 der Pfad zu den Logdateien von `/var/log/httpd` in `/var/log/apache2` geändert werden. Für die Domain, die der Server ursprünglich gehostet hat (`www.meinefirma.de`), muss dabei ebenfalls ein VirtualHost-Eintrag angelegt werden. In diesem

Beispiel wird also die ursprüngliche Domain und zusätzlich eine weitere Domain (`www.meineanderefirma.de`) auf demselben Server gehostet.

In den `VirtualHost`-Direktiven wird wie bei `NameVirtualHost` ebenfalls ein * angegeben. Den Zusammenhang zwischen der Anfrage und dem Virtual Host stellt Apache über das Host-Feld im HTTP-Header her. Die Anfrage wird an den Virtual Host weitergeleitet, dessen `ServerName` mit dem in diesem Feld angegebenen Hostnamen übereinstimmt.

Bei den Direktiven `ErrorLog` und `CustomLog` ist es nicht entscheidend, dass die Log-Dateien den Domain-Namen enthalten, man kann hier beliebige Namen verwenden.

`ServerAdmin` benennt die E-Mail-Adresse eines Verantwortlichen, an den man sich bei Problemen wenden kann. Treten Fehler auf, dann gibt Apache diese Adresse in Fehlermeldungen an, die er an den Client zurückschickt.

22.10.2 IP-basierte Virtual Hosts

Für diese Alternative muss man auf einem Rechner mehrere IPs einrichten. Eine Instanz von Apache bedient dann mehrere Domains, wobei jede Domain einer IP zugewiesen ist. Das folgende Beispiel zeigt, wie man Apache so einrichtet, dass er außer auf seiner ursprünglichen IP `192.168.1.10` noch zwei weitere Domains auf zusätzlichen IPs (`192.168.1.20` und `192.168.1.21`) hostet. Dieses konkrete Beispiel funktioniert natürlich nur in einem Intranet, da IPs aus dem Bereich von `192.168.0.0` bis `192.168.255.0` im Internet nicht weitergeleitet (geroutet) werden.

IP-Aliasing einrichten

Damit Apache mehrere IPs hosten kann, muss der Rechner, auf dem er läuft, Anfragen für mehrere IPs akzeptieren. Dies bezeichnet man auch als Multi-IP-Hosting. Dazu muss als erstes IP-Aliasing im Kernel aktiviert sein. Dies ist bei SUSE LINUX standardmäßig der Fall.

Ist der Kernel für IP-Aliasing konfiguriert, kann man mit den Befehlen `ifconfig` und `route` weitere IPs auf dem Rechner einrichten. Um diese Kommandos einzugeben, muss man als `root` eingeloggt sein. Im Folgenden wird angenommen, dass der Rechner bereits eine eigene IP-Adresse, zum Beispiel `192.168.1.10` hat, die dem Netzwerkdevice `eth0` zugewiesen ist.

Welche IP der Rechner verwendet, lässt sich durch Eingabe von `ifconfig` feststellen. Weitere IPs fügt man dann zum Beispiel auf folgende Weise hinzu:

```
/sbin/ifconfig eth0:0 192.168.1.20
/sbin/ifconfig eth0:1 192.168.1.21
```

Alle diese IPs sind dann demselben physikalischen Netzwerkdevice (`eth0`) zugewiesen.

Virtual Hosts mit IPs

Ist IP-Aliasing auf dem System eingerichtet oder der Rechner mit mehreren Netzwerkkarten konfiguriert worden, kann man Apache konfigurieren. Für jeden virtuellen Server gibt man einen eigenen `VirtualHost`-Block an:

```
<VirtualHost 192.168.1.20>
    ServerName www.meineanderefirma.de
    DocumentRoot /srv/www/htdocs/meineanderefirma.de
    ServerAdmin webmaster@meineanderefirma.de
    ErrorLog /var/log/httpd/www.meineanderefirma.de-error_log
    CustomLog /var/log/httpd/www.meineanderefirma.de-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.nocheinefirma.de
    DocumentRoot /srv/www/htdocs/nocheinefirma.de
    ServerAdmin webmaster@nocheinefirma.de
    ErrorLog /var/log/httpd/www.nocheinefirma.de-error_log
    CustomLog /var/log/httpd/www.nocheinefirma.de-access_log common
</VirtualHost>
```

Hier werden VirtualHost-Direktiven nur für die zusätzlichen Domains angegeben, die ursprüngliche Domain (`www.meinefirma.de`) wird nach wie vor über die entsprechenden Einstellungen (`DocumentRoot` etc.) außerhalb der `VirtualHost`-Blöcke konfiguriert.

22.10.3 Mehrere Instanzen von Apache

Bei den vorhergehenden Methoden für Virtual Hosts können die Administratoren einer Domain die Daten der anderen Domains lesen. Will man die einzelnen Domains voneinander abschotten, kann man mehrere Instanzen von Apache starten, die jeweils eigene Einstellungen für `User`, `Group` etc. in der Konfigurationsdatei verwenden.

In der Konfigurationsdatei gibt man mit der `Listen` Direktive an, für welche IP die jeweilige Instanz von Apache zuständig ist. Analog zum vorhergehenden Beispiel lautet diese Direktive dann für die erste Instanz von Apache:

```
Listen 192.168.1.10:80
```

Für die anderen beiden Instanzen jeweils:

```
Listen 192.168.1.20:80
Listen 192.168.1.21:80
```

22.11 Sicherheit

22.11.1 Das Risiko gering halten

Wenn man auf einem Rechner keinen Webserver benötigt, sollte man Apache im Runlevel-Editor deaktivieren oder erst gar nicht installieren bzw. deinstallieren. Jeder Server, der auf einem Rechner nicht läuft, ist eine Angriffmöglichkeit weniger. Dies gilt insbesondere für Rechner, die als Firewalls dienen, auf diesen sollten grundsätzlich nach Möglichkeit keine Server laufen.

22.11.2 Zugriffsrechte

DocumentRoot sollte Root gehören

Per Voreinstellung gehört das Verzeichnis `DocumentRoot` (`/srv/www/htdocs`) und das CGI-Verzeichnis dem Benutzer `root`. Das sollte man auch so belassen. Sind diese Verzeichnisse für jedermann beschreibbar, kann dort jeder Benutzer Dateien ablegen. Diese Dateien werden dann von Apache ausgeführt, und zwar als Benutzer `wwwrun`. Apache sollte keine Schreibrechte auf die Daten und Skripte haben, die er ausliefert. Deshalb sollten diese nicht dem Benutzer `wwwrun`, sondern zum Beispiel `root` gehören.

Möchte man Usern die Möglichkeit geben, Dateien im Dokument-Verzeichnis von Apache unterzubringen, so sollte man, anstatt dieses für alle beschreibbar zu machen, ein für alle beschreibbares Unterverzeichnis einrichten, zum Beispiel `/srv/www/htdocs/wir_ueber_uns`.

Dokumente aus dem eigenen Home-Verzeichnis veröffentlichen

Eine weitere Möglichkeit dafür zu sorgen, dass Anwender eigene Dateien ins Netz stellen können ist, in der Konfigurationsdatei ein Verzeichnis im Home des Users anzugeben, in dem dieser seine Dateien für die Web-Präsentation ablegen kann (zum Beispiel `~/public_html`). Dies ist bei SUSE LINUX per Voreinstellung aktiviert, die Einzelheiten sind im Abschnitt 22.7.2 auf Seite 594 beschrieben.

Auf diese Webseiten kann dann unter Angabe des Users in der URL zugegriffen werden, die URL enthält die Bezeichnung ⟨ *username*⟩ als Kürzel für das entsprechende Verzeichnis im Home-Verzeichnis des Anwenders. Ein Beispiel: Die Eingabe der URL `http://localhost/~tux` in einem Browser zeigt die Dateien aus dem Verzeichnis `public_html` im Home-Verzeichnis des Anwenders tux an.

22.11.3 Immer auf dem Laufenden bleiben

Wer einen Webserver betreibt sollte, besonders wenn dieser Webserver öffentlich verfügbar ist, immer auf dem neuesten Stand bleiben, was Fehler und die dadurch möglichen Angriffsflächen angeht.

Quellen für die Recherche nach Exploits und Fixes sind im Abschnitt 22.13.3 auf Seite 608 aufgelistet.

22.12 Troubleshooting

Sollten Probleme auftreten, etwa dass Apache eine Seite gar nicht oder nicht korrekt anzeigt, helfen Ihnen folgende Maßnahmen beim Ermitteln der Fehlerquelle.

- Schauen Sie zunächst in der Fehler-Logdatei nach, ob aus den Meldungen darin hervorgeht, was schiefläuft: `/var/log/httpd/error_log` bzw. `/var/log/apache2/error_log`.

  Lassen Sie idealerweise in einer Konsole die Logfiles anzeigen, um während der Zugriffe auf den Server parallel mitlesen zu können, wie er reagiert. Geben Sie dazu in einer `root`-Konsole folgenden Befehl ein:`tail -f /var/log/apache2/*_log`.

- Schauen Sie in der Bug-Datenbank nach. Diese ist online unter `http://bugs.apache.org/` verfügbar.

- Lesen Sie die Mailinglisten und Newsgroups. Die Mailingliste für Anwender findet man unter `http://httpd.apache.org/userslist.html`. Als Newsgroup emfehlen sich `comp.infosystems.www.servers.unix` und verwandte Gruppen.
- Wenn alle vorhergehenden Möglichkeiten keine Lösung gebracht haben und Sie sich sicher sind, dass Sie einen Bug in Apache gefunden haben, dann können Sie diesen unter `http://www.suse.de/feedback/` an uns direkt melden.

22.13 Weitere Dokumentation

22.13.1 Apache

Apache kommt mit einer ausführlichen Dokumentation. Wie man diese installiert, ist im Abschnitt 22.6 auf Seite 587 beschrieben. Sie steht dann unter `http://localhost/manual` zur Verfügung. Die aktuellste Dokumentation findet man natürlich immer auf der Homepage von Apache: `http://httpd.apache.org`

22.13.2 CGI

Weitere Informationen zu CGI bieten folgende Seiten:

- `http://apache.perl.org/`
- `http://perl.apache.org/`
- `http://www.modperl.com/`
- `http://www.modperlcookbook.org/`
- `http://www.fastcgi.com/`
- `http://www.boutell.com/cgic/`

22.13.3 Sicherheit

Unter `http://www.suse.de/security/` werden laufend die aktuellen Patches für die SUSE Pakete zur Verfügung gestellt. Diese URL sollten Sie regelmäßig besuchen, dort können Sie auch die SUSE Security Announcements per Mailingliste abonnieren.

Das Apache-Team betreibt eine offene Informationspolitik, was Fehler in Apache angeht. Aktuelle Meldungen über Bugs und dadurch mögliche Angriffsstellen findet man unter `http://httpd.apache.org/security_report.html`.

Hat man selber ein Sicherheitsproblem entdeckt (bitte erst auf den eben genannten Seiten verifizieren, ob es wirklich neu ist), kann man es per Mail an `security@suse.de` oder auch `security@apache.org` melden.

Weitere Quellen für Informationen über Sicherheitsprobleme bei Apache (und anderen Internet-Programmen) sind:

- `http://www.cert.org/`
- `http://www.vnunet.com/`
- `http://www.securityfocus.com/`

Eine deutsche Seite zum Thema Sicherheit ist die Heise Security Liste `http://www.heisec.de/`

22.13.4 Weitere Quellen

Es empfiehlt sich, bei Schwierigkeiten einen Blick in die SUSE Support-Datenbank zu werfen: `http://sdb.suse.de/`

Eine Online-Zeitung rund um Apache gibt es unter der URL: `http://www.apacheweek.com/`

Die Enstehungsgeschichte von Apache wird unter `http://httpd.apache.org/ABOUT_APACHE.html` beschrieben. Hier erfährt man auch, warum der Server eigentlich Apache heisst.

Informationen über den Upgrade von Version 1.3 auf 2.0 findet man unter `http://httpd.apache.org/docs-2.0/de/upgrading.html`.

Datei-Synchronisation

Viele Menschen benutzen heutzutage mehrere Computer. Ein Computer zu Hause, ein oder mehrere Rechner am Arbeitsplatz und eventuell noch einen Laptop oder PDA für unterwegs. Viele Dateien benötigt man auf allen Computern und möchte sie auch bearbeiten. Dennoch sollen alle Daten überall in aktueller Version zur Verfügung stehen.

23.1 Software zur Datensynchronisation 610
23.2 Kriterien für die Programmauswahl 612
23.3 Einführung unison 616
23.4 Einführung CVS 618
23.5 Einführung in subversion 622
23.6 Einführung in rsync 625
23.7 Einführung mailsync 627

23.1 Software zur Datensynchronisation

Auf Computern, die ständig miteinander über ein schnelles Netzwerk in Verbindung stehen, ist die Datensynchronisation kein Problem. Man wählt ein Netzwerkdateisystem, wie zum Beispiel NFS, und speichert die Dateien auf einem Server. Alle Rechner greifen dabei über das Netzwerk auf ein und dieselben Daten zu.

Dieser Ansatz ist unmöglich, wenn die Netzverbindung schlecht oder teilweise gar nicht vorhanden ist. Wer mit einem Laptop unterwegs ist, ist darauf angewiesen, von allen benötigten Dateien Kopien auf der lokalen Festplatte zu haben. Wenn Dateien bearbeitet werden stellt sich aber schnell das Problem der Synchronisierung. Wird auf einem Computer eine Datei verändert, muss man tunlichst aufpassen, dass man die Kopie der Datei auf allen anderen Rechnern auch aktualisiert. Dies kann bei seltenen Kopiervorgängen von Hand mit Hilfe von scp oder rsync erledigt werden. Bei vielen Dateien wird das schnell aufwändig und erfordert hohe Aufmerksamkeit vom Benutzer, um Fehler, wie zum Beispiel das Überschreiben einer neuen mit einer alten Datei, zu vermeiden.

Achtung

Datenverlust droht

Man sollte in jedem Fall sich mit dem verwendeten Programm vertraut machen und seine Funktion testen, bevor man seine Daten über ein Synchronisationssystem verwaltet. Für wichtige Dateien ist ein Backup unerlässlich.

Achtung

Um diese zeitraubende und fehlerträchtige Handarbeit der Datensynchronisation zu vermeiden, gibt es Software, die mit verschiedenen Ansätzen diese Arbeit automatisiert. Die folgenden Kurzeinführungen sollen dem Nutzer eine Vorstellung davon liefern, wie diese Programme funktionieren und genutzt werden können. Vor dem tatsächlichen Einsatz empfehlen wir, die Programmdokumentation sorgfältig zu lesen.

23.1.1 unison

Bei unison handelt es sich nicht um ein Netzwerkdateisystem. Stattdessen werden Dateien ganz normal lokal gespeichert und bearbeitet. Von Hand

kann das Programm unison aufgerufen werden, um Dateien zu synchronisieren. Beim ersten Abgleich wird auf den beteiligten zwei Computern eine Datenbank angelegt, in der Prüfsummen, Zeitstempel und Berechtigungen der ausgewählten Dateien gespeichert sind.

Beim nächsten Aufruf kann unison erkennen, welche Dateien verändert wurden und die Übertragung vom oder zum anderen Rechner vorschlagen. Im besten Fall kann man alle Vorschläge annehmen.

23.1.2 CVS

Meist zur Versionsverwaltung von Quelltexten von Programmen benutzt bietet CVS die Möglichkeit, Kopien der Dateien auf mehreren Computern zu haben. Damit eignet es sich auch für unseren Zweck.

Bei CVS gibt es eine zentrale Datenbank (repository) auf dem Server, welche nicht nur die Dateien, sondern auch die Veränderungen an ihnen abspeichert. Veränderungen, die man lokal durchführt, werden in die Datenbank eingecheckt (commit) und können von anderen Computern wieder abgeholt werden (update). Beides muss vom Benutzer initiiert werden.

Dabei ist CVS bei Veränderungen auf mehreren Computern sehr fehlertolerant: Die Veränderungen werden zusammengeführt und nur wenn in den gleichen Zeilen Veränderungen stattfanden, gibt es einen Konflikt. Die Datenbank bleibt im Konfliktfall in einem konsistenten Zustand und der Konflikt ist nur auf dem Client Computer sichtbar und zu lösen.

23.1.3 subversion

Im Gegensatz zum gewachsenen CVS ist subversion ein durchgängig konzipiertes Projekt; subversion wurde entwickelt um CVS abzulösen, und dessen technische Limitierungen aufzuheben.

subversion wurde in vielen Bereichen zu seinem Vorgänger deutlich verbessert. CVS verwaltet aufgrund seiner Geschichte nur Dateien und „weiß“ nichts von Verzeichnissen. In subversion dagegen, besitzen auch Verzeichnisse eine Versionshistorie und können genauso wie Dateien kopiert und umbenannt werden. Des Weiteren kann zu jeder Datei und zu jedem Verzeichnis Metadateien hinzugefügt werden, die ebenfalls der Versionsverwaltung unterliegen. Im Gegensatz zu CVS bietet subversion transparenten Netzwerkzugriff über einige Protokolle wie zum Beispiel WebDAV.

Zur Realisierung von subversion wurde weitgehend auf existierende Programmpakete zurückgegriffen. So wird zum Betrieb von subversion immer auch der Webserver apache mit der Erweiterung WebDAV verwendet.

23.1.4 mailsync

Im Vergleich zu den bisher erwähnten Synchronisationswerkzeugen dient Mailsync einzig und allein der Aufgabe, E-Mails zwischen Mailboxen zu synchronisieren. Es kann sich sowohl um lokale Mailbox-Dateien als auch um Mailboxen handeln, die auf einem IMAP-Server untergebracht sind.

Dabei wird für jede Nachricht aufgrund der im E-Mail-Header enthaltenen Message-ID einzeln entschieden, ob sie synchronisiert bzw. gelöscht werden muss. Es ist sowohl die Synchronisation zwischen einzelnen Mailboxen, als auch zwischen Hierarchien von Mailboxen möglich.

23.1.5 rsync

Wenn Sie keine Versionskontrolle benötigen, und grosse Dateibäume über langsame Netzwerkverbindungen synchronisieren möchten, bietet sich das Tool rsync an. rsync verfügt über ausgefeilte Mechanismen, um ausschließlich Änderungen an Dateien zu übertragen. Dies betrifft nicht nur Textdateien sondern auch binäre Dateien. Um die Unterschiede zwischen Dateien zu erkennen, teilt rsync die Dateien in Blöcke auf, und berechnet Prüfsummen zu diesen Blöcken.

Der Aufwand, der zum Erkennen der Änderungen betrieben wird hat auch seinen Preis. Zum Betrieb von rsync sollte man die Rechner, die synchronisiert werden sollen, großzügig dimensionieren. Vor allem am RAM sollte nicht gespart werden.

23.2 Kriterien für die Programmauswahl

23.2.1 Client-Server-Modell versus Gleichberechtigung

Zur Verteilung von Daten sind zwei verschiedene Modelle verbreitet. Einerseits kann man einen zentralen Server verwenden, mit dem alle anderen

Computer (sog. Clients) ihre Dateien abgleichen. Der Server muss dann zumindest zeitweise über ein Netzwerk von allen Clients erreichbar sein. Dieses Modell wird von subversion, CVS und WebDAV verwendet. Andererseits können alle Computer gleichberechtigt vernetzt sein und ihre Daten gegenseitig abgleichen. Diesen Ansatz verfolgt unison. rsync arbeitet eigentlich im Client-Server Betrieb, jedoch kann jeder Client auch wieder als Server verwendet werden.

23.2.2 Portabilität

Subversion, CVS, rsync und unison sind auch auf vielen anderen Betriebssystemen wie anderen Unices und Windows erhältlich.

23.2.3 Interaktiv versus Automatisch

Bei subversion, CVS, WebDAV, rsync und unison wird der Datenabgleich manuell vom Benutzer angestoßen. Dies erlaubt die genaue Kontrolle über die abzugleichenden Dateien und einen einfachen Umgang mit Konflikten. Andererseits kann es leicht passieren, dass der Abgleich zu selten durchgeführt wird, wodurch sich die Chancen auf einen Konflikt erhöhen.

23.2.4 Konflikte: Auftreten und Lösung

Konflikte treten bei subversion oder CVS nur selten auf, selbst wenn mehrere Leute an einem großen Programmprojekt arbeiten. Die Dokumente werden hier zeilenweise zusammengeführt. Wenn ein Konflikt auftritt, dann ist davon immer nur ein Client betroffen. In der Regel sind Konflikte mit subversion oder CVS einfach zu lösen. Bei unison bekommt man Konflikte mitgeteilt und kann die Datei einfach vom Abgleich ausnehmen. Änderungen lassen sich aber nicht so einfach zusammenführen wie bei subversion oder CVS.

Während in subversion oder CVS im Konfliktfall Änderungen auch teilweise übernommen werden können, wird bei WebDAV ein checkin nur dann vollzogen, wenn die gesamte Änderung erfolgreich ist.

In rsync gibt es keine Konfliktbehandlung. Der Benutzer muss selbst darauf achten, dass er nicht versehentlich Dateien überschreibt, und alle eventuell auftauchenden Konflikte von Hand lösen. Um sicher zu gehen, kann man zusätzlich ein Versionierungssystem wie RCS verwenden.

23.2.5 Dateiwahl, Dateien hinzufügen

Bei unison und rsync werden ganze Verzeichnisbäume synchronisiert. Dort neu erscheinende Dateien werden auch automatisch in die Synchronisation mit einbezogen.

Bei subversion oder CVS müssen neue Verzeichnisse und Dateien explizit mittels `svn add` bzw. `cvsadd` hinzugefügt werden. Daraus resultiert eine genauere Kontrolle über die zu synchronisierenden Dateien. Andererseits werden neue Dateien gerne vergessen, vor allem, wenn aufgrund der Anzahl der Dateien die '?' in der Ausgabe von `svn update`, `svn status` bzw. `cvs update` ignoriert werden.

23.2.6 Geschichte

Subversion oder CVS bietet eine Rekonstruktion alter Dateiversionen als zusätzliches Feature. Bei jeder Veränderung kann man einen kurzen Bearbeitungsvermerk hinzufügen und später die Entwicklung der Dateien aufgrund des Inhalts und der Vermerke gut nachvollziehen. Für Diplomarbeiten und Programmtexte ist dies eine wertvolle Hilfe.

23.2.7 Datenmenge / Plattenbedarf

Auf jedem der beteiligten Computer benötigt man für alle verteilten Daten genügend Platz auf der Festplatte. Bei subversion bzw. CVS fällt zusätzlich der Platzbedarf für die Datenbank (dem *repository*) auf dem Server an. Da dort auch die Geschichte der Dateien gespeichert wird, ist dieser deutlich größer als der reine Platzbedarf. Bei Dateien im Textformat hält sich dies in Grenzen, da nur geänderte Zeilen neu gespeichert werden müssen. Bei binären Dateien wächst hingegen der Platzbedarf bei jeder Änderung um die Größe der Datei.

23.2.8 GUI

unison kommt mit einer grafischen Oberfläche, die anzeigt, welche Abgleiche unison vornehmen möchte. Man kann den Vorschlag annehmen oder einzelne Dateien vom Abgleich ausnehmen. Daneben kann man auch im Textmodus interaktiv die einzelnen Vorgänge bestätigen.

Subversion bzw. CVS wird von erfahrenen Benutzern normalerweise an der Kommandozeile benutzt. Es gibt jedoch grafische Oberflächen für Linux (cervisia, ...) und auch für Windows (wincvs). Viele Entwicklungstools (zum Beispiel kdevelop) und Texteditoren (zum Beispiel emacs)

haben eine Unterstützung für CVS oder subversion. Die Behebung von Konflikten wird mit diesen Frontends oft sehr vereinfacht.

23.2.9 Anforderungen an den Benutzer

unison und rsync sind recht einfach zu benutzen und bieten sich auch für Anfänger an. CVS oder subversion sind etwas schwieriger zu benutzen. Man sollte zu dessen Verwendung das Zusammenspiel zwischen Repository, und lokalen Daten verstanden haben. Veränderungen an den Daten sollten zunächst immer lokal mit dem Repository zusammengeführt werden. Hierzu dient der Befehl `cvs update` bzw. `svn update`. Nachdem dies geschehen ist, müssen die Daten mit dem Befehl `cvs commit` bzw. `svn commit` wieder in das Repository zurückgeschickt werden. Wenn man dies verinnerlicht hat, ist CVS bzw. subversion auch für Anfänger leicht zu benutzen.

23.2.10 Sicherheit gegen Angriffe

Die Sicherheit bei der Übertragung der Daten gegenüber Abhören oder gar Verändern der Daten sollte idealerweise gewährleistet werden.

Sowohl unison als auch CVS, rsync oder subversion lassen sich einfach über ssh (Secure Shell) benutzen und sind dann gut gegen obige Angriffe gesichert. Es sollte vermieden werden, CVS oder unison über rsh (Remote Shell) einzusetzen und auch Zugriffe über den CVS pserver Mechanismus sind in ungeschützten Netzwerken nicht empfehlenswert. subversion bietet hier schon von Haus aus durch die Verwendung des Apache die notwendigen Sicherheitsmechanismen an.

23.2.11 Sicherheit gegen Datenverlust

CVS wird schon sehr lange von vielen Entwicklern zur Verwaltung ihrer Programmprojekte benutzt und ist ausgesprochen stabil. Durch das Speichern der Entwicklungsgeschichte ist man bei CVS sogar gegen gewisse Benutzerfehler (zum Beispiel irrtümlichen Löschen einer Datei) geschützt. Obwohl subversion im Vergleich zu CVS noch nicht sehr häufig verbreitet ist, wird sie bereits im produktiven Einsatz verwendet (zum Beispiel vom Subversion-Projekt selbst).

unison ist noch relativ neu, aber weist eine hohe Stabilität auf. Es ist empfindlicher gegen Benutzerfehler. Wenn man der Synchronisierung eines Löschvorgangs bei einer Datei einmal zustimmt, ist diese nicht mehr zu retten. Die selbe Problematik trifft auch auf rsync zu.

Tabelle 23.1: *Features der Datensynchronisationstools: -- = sehr schlecht, - = schlecht bzw. nicht vorhanden, o = mittelmäßig, + = gut, ++ = sehr gut, x = vorhanden*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Client/Server	gleich	C-S/C-S	C-S	gleich
Portabil.	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interaktiv	x	x/x	x	-
Geschwind.	-	o/+	+	+
Konflikte	o	++/++	o	+
Dateiwahl	Verzeichnis	Ausw./Datei,Verz.	Verzeichnis	Mailbox
Geschichte	-	x/x	-	-
Plattenbed.	o	--	o	+
GUI	+	o/o	-	-
Schwierigk.	+	o/o	+	o
Angriffe	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Datenverlust	+	++/++	+	+

23.3 Einführung unison

23.3.1 Einsatzgebiete

Unison ist hervorragend für den Abgleich und Transfer ganzer Verzeichnisbäume geeignet. Der Abgleich findet in beide Richtungen statt und lässt sich intuitiv über ein grafisches Frontend steuern (alternativ kann aber auch die Konsolen-Version verwenden). Der Abgleich lässt sich auch automatisieren (das heißt keine Interaktion mit dem Benutzer), wenn man weiß, was man tut.

23.3.2 Voraussetzungen

Unison muss sowohl auf dem Client, als auch auf dem Server installiert sein, wobei mit Server ein zweiter, entfernter Rechner gemeint ist (im Gegensatz zu CVS, siehe Abschnitt 23.1.2 auf Seite 611).

Da wir uns im Folgenden auf die Benutzung von unison mit ssh beschränken, muss ein ssh-Client auf dem Client und ein ssh-Server auf dem Server installiert sein.

23.3.3 Bedienung

Das Grundprinzip bei Unison ist, zwei Verzeichnisse (so genannte "roots") aneinander zu binden. Diese Bindung ist symbolisch zu verstehen, es handelt sich also nicht um eine Online-Verbindung. Angenommen, wir haben folgendes Verzeichnis-Layout:

Client:	`/home/tux/dir1`
Server:	`/home/geeko/dir2`

Diese beiden Verzeichnisse sollen synchronisiert werden. Auf dem Client ist der User als tux bekannt, auf dem Server dagegen als `geeko`. Zunächst sollte ein Test durchgeführt werden, ob die Kommunikation zwischen Client und Server funktioniert:

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Die häufigsten Probleme, die hierbei auftreten können:

- die auf dem Client und Server eingesetzten Versionen von unison sind nicht kompatibel
- der Server lässt keine SSH-Verbindung zu
- keiner der beiden angegebenen Pfade existiert

Funktioniert soweit alles, lässt man die Option `-testserver` weg. Bei der Erstsynchronisierung kennt unison das Verhältnis der beiden Verzeichnisse noch nicht und macht von daher Vorschläge für die Transferrichtung der einzelnen Dateien und Verzeichnisse. Die Pfeile in der Spalte Action geben die Transferrichtung an. Ein '?' bedeutet, dass unison keinen Vorschlag bzgl. der Transferrichtung machen kann, da beide Versionen in der Zwischenzeit verändert wurden bzw. neu sind.

Mit den Pfeiltasten kann man die Transferrichtung für jeden Eintrag einstellen. Stimmen die Transferrichtungen für alle angezeigten Einträge, dann klickt man auf 'Go'.

Das Verhalten von unison (zum Beispiel ob in eindeutigen Fällen die Synchronisation automatisch durchgeführt werden soll), lässt sich beim Starten per Kommandozeilenparameter steuern. Eine komplette Liste aller Parameter liefert `unison -help`.

Über die Synchronisation wird für jede Bindung im Benutzer-Verzeichnis `~/.unison` Protokoll geführt. In diesem Verzeichnis lassen sich auch Konfigurationssets ablegen, zum Beispiel `~/.unison/example.prefs`:

Beispiel 23.1: *Die Datei /.unison/example.prefs*

```
root=/home/foobar/dir1
root=ssh://fbar@server//homes/fbar/dir2
batch=true
```

Um die Synchronisation anzustoßen, genügt es dann einfach, diese Datei als Kommandozeilenargument anzugeben: `unison example.prefs`

23.3.4 Weiterführende Literatur

Die offizielle Dokumentation zu unison ist äußerst umfangreich; in diesem Abschnitt wurde nur eine Kurzeinführung dargestellt. Unter `http://www.cis.upenn.edu/~bcpierce/unison/` bzw. im SUSE-Paket `unison` ist ein komplettes Handbuch verfügbar.

23.4 Einführung CVS

23.4.1 Einsatzgebiete

CVS bietet sich zur Synchronisation an, wenn einzelne Dateien häufig bearbeitet werden und in einem Dateiformat vorliegen wie ASCII-Text oder Programmquelltext. Die Verwendung von CVS für die Synchronisation von Daten in anderen Formaten (zum Beispiel JPEG-Dateien) ist zwar möglich, führt aber schnell zu großen Datenmengen, da jede Variante einer Datei dauerhaft auf dem CVS-Server gespeichert wird. Zudem bleiben in solchen Fällen die meisten Möglichkeiten von CVS ungenutzt.

Die Verwendung von CVS zur Dateisynchronisation ist nur dann möglich, wenn alle Arbeitsplatzrechner auf denselben Server zugreifen können!

Im Gegensatz dazu wäre zum Beispiel mit dem Programm unison auch folgendes Szenario möglich:

A > B > C > S

A, B, C sind Rechner, die die fraglichen Daten bearbeiten können.

23.4.2 Einrichten eines CVS-Servers

Der Server ist der Ort, wo alle gültigen Dateien liegen, d. h. insbesondere die aktuelle Version jeder Datei. Als Server kann zum Beispiel ein fest installierter Arbeitsplatzrechner dienen. Wünschenswert ist, dass die Daten des CVS-Servers regelmäßig in ein Backup mit einbezogen werden.

Ein sinnvoller Weg, einen CVS-Server aufzusetzen, ist, dem Benutzer Zugang per SSH auf den Server zu gestatten. So kann zum Beispiel ein fest installierter Arbeitsplatzrechner als Server dienen.

Ist auf diesem Server der Benutzer als tux bekannt und sowohl auf dem Server als auch auf dem Client (zum Beispiel Notebook) die CVS-Software installiert, sollte man auf der Client-Seite dafür Sorge tragen, dass folgende Umgebungsvariablen gesetzt sind:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

Mit dem Befehl `cvs init` lässt sich dann von der Client-Seite aus der CVS-Server initialisieren (dies muss nur einmal geschehen).

Abschließend muss ein Name für die Synchronisation festgelegt werden. Wählen oder erzeugen Sie auf einem Client ein Verzeichnis, das ausschließlich Dateien enthält, die von CVS verwaltet werden sollen (es kann auch leer sein). Der Name des Verzeichnisses spielt dabei keine Rolle und soll in diesem Beispiel `synchome` sein. Wechseln Sie in dieses Verzeichnis. Um den Synchronisationsnamen auf `synchome` zu setzen, gibt man Folgendes ein:

```
cvs import synchome tux tux_0
```

Hinweis: Viele Kommandos von CVS verlangen einen Kommentar. Zu diesem Zweck ruft CVS einen Editor auf (den in der Umgebungsvariable `$EDITOR` definierten, ansonsten vi). Den Aufruf des Editors kann man umgehen, indem man den Kommentar bereits auf der Kommandozeile angibt, wie zum Beispiel in

```
cvs import -m 'dies ist ein Test' synchome tux tux_0
```

23.4.3 Benutzung von CVS

Ab diesem Zeitpunkt kann das Synchronisationsrepository von beliebigen Rechnern ausgecheckt werden:

```
cvs co synchome
```

Man erhält dadurch ein neues Unterverzeichnis `synchome` auf dem Client. Hat man Änderungen durchgeführt, die man an den Server übermitteln will, so wechselt man in das synchome-Verzeichnis (oder auch ein Unterverzeichnis desselben) und gibt folgenden Befehl ein:

```
cvs commit
```

Dabei werden standardmäßig alle Dateien, die unterhalb des aktuellen Verzeichnisses liegen, und zum lokalen CVS gehören an den Server übermittelt. Will man nur einzelne Dateien oder Verzeichnisse übermitteln, so muss man diese angeben:

```
cvs commit datei1 ... verzeichnis1 ...
```

Neue Dateien/Verzeichnisse muss man vor der Übermittlung an den Server als dem CVS zugehörig deklarieren:

```
cvs add datei1 ... verzeichnis1 ...
```

und danach übermitteln

```
cvs commit datei1 ... verzeichnis1 ...
```

Wechselt man nun den Arbeitsplatz, sollte, falls dies nicht schon in früheren Sessions am gleichen Arbeitsplatz geschehen ist, das Synchronisationsrepository ausgecheckt werden. Der Abgleich mit dem Server wird über das Kommando angestoßen:

```
cvs update
```

Man kann auch selektiv Dateien/Verzeichnisse updaten:

```
cvs update datei1 ... verzeichnis1 ...
```

Will man im voraus die Unterschiede zu den auf dem Server gespeicherten Versionen sehen, so geht dies mit dem Befehl `cvs diff` oder explizit mit:

```
cvs diff datei1 ... verzeichnis1 ...
```

Alternativ kann man sich auch anzeigen lassen, welche Dateien von einem Update betroffen wären: `cvs -nq update`. Bei einem Update werden (u. a.) folgende Status-Symbole verwendet:

U Die lokale Version wurde auf den neuesten Stand gebracht. Dies betrifft alle Dateien, die der Server bereitstellt, die aber nicht lokal existierten.

M Die lokale Version wurde modifiziert. Soweit sich diese auf dem Server verändert hat, konnten die Änderungen auch lokal eingepflegt werden.

P Die lokale Version wurde mit Hilfe eines Patches auf den aktuellen Stand gebracht.

? Diese Datei ist nicht im CVS.

Der Status `M` markiert Dateien, die gerade bearbeitet werden. Um die Änderungen zum Server zurückzusenden, muss man den Befehl `cvs commit` ausführen. Wenn man stattdessen auf die eigenen Änderungen verzichten möchte, um den aktuellen Stand des Servers zu übernehmen, entfernt man die lokale Kopie, und führt erneut ein Update durch. Die fehlende Datei wird dann vom Server geholt.

Wenn von verschiedenen Benutzern die gleiche Datei an derselben Stelle editiert wurde, entsteht eine Situation, in der CVS nicht entscheiden kann, welche Version verwendet werden soll. Dieser Fall wird bei einem Update mit dem Symbol `C` gekennzeichnet. Zur Lösung eine Konfliktes bieten sich verschiedene Vorgehensweisen an. In der entsprechenden Datei werden an den betreffenden Stellen Konfliktmarken eingefügt, die manuell editiert werden können. Für Anfänger ist es empfehlenswert, in diesem Fall auf ein Hilfsprogramm wie cervisia zurückzugreifen. Alternativ kann man auch die eigene Datei umbenennen und erneut ein Update ausführen. Sobald man die Änderungen an der aktuellen Datei beendet hat, sollte man diese dem Server mit dem Befehl `cvs commit` übergeben. Dadurch wird die Wahrscheinlichkeit für Konflikte reduziert.

23.4.4 Weiterführende Literatur

Die Möglichkeiten von CVS sind umfangreich und es konnte hier nur ein kleiner Einblick gegeben werden. Weiterführende Dokumentation gibt es unter anderem unter `http://www.cvshome.org/` und `http://www.gnu.org/manual/`.

23.5 Einführung in subversion

23.5.1 Einsatzgebiete

Subversion ist ein freies Open Source Versionskontrollsystem und wird häufig als Nachfolger von CVS gehandelt; somit treffen bereits vorgestellte Eigenschaften von CVS auch auf subversion zum großen Teil zu. Es bietet sich vor allem an, wenn man die Vorteile von CVS genießen möchte, ohne gleich dessen Nachteile in Kauf nehmen zu müssen. Viele dieser Eigenschaften wurden bereits ansatzweise in Abschnitt 23.1.3 auf Seite 611 vorgestellt.

23.5.2 Einrichten eines Subversion-Servers

Das Einrichten eines Repository auf einem Server ist eine recht einfache Prozedur. Hierzu stellt subversion ein eigenes Administrationstool, `svnadmin`, zur Verfügung. Um ein neues Repository zu erstellen, gibt man ein:

```
svnadmin create /pfad/zum/repository
```

Weitere Optionen erhalten Sie mit `svnadmin help`. Im Gegensatz zu CVS verwendet subversion nicht RCS als Basis, sondern die Berkeley Datenbank. Achten Sie darauf, ein Repository *nicht* auf entfernten Dateisystemen wie NFS, AFS oder Windows SMB anzulegen. Die Datenbank benötigt POSIX Lockingmechanismen, welche die genannten Dateisysteme nicht bieten.
Um den Inhalt eines existierenden Repositories einzusehen, gibt es den Befehl `svnlook`:

```
svnlook info /pfad/zum/repository
```

Damit andere Benutzer auf das Repository zugreifen können, muss ein Server konfiguriert werden. Hierbei kann auf den Webserver Apache zurückgegriffen werden oder man verwendet den hauseigenen Server von subversion, `svnserve`. Läuft `svnserve` einmal, kann über das Schema `svn://` oder `svn+ssh://` in einer URL auf das Repository zugegriffen werden. Über die Konfigurationsdatei `/etc/svnserve.conf` können Sie Benutzer einstellen, die sich dann beim Aufruf von `svn` authentifizieren müssen.
Die Entscheidung für oder gegen den einen oder anderen hängt von vielen Faktoren ab. Hier empfiehlt sich ein Blick in das subversion-Buch (Informationen hierzu, siehe Abschnitt 23.5.4 auf Seite 625).

23.5.3 Benutzung

Um auf ein Subversion-Repository zuzugreifen, gibt es den Befehl `svn` (ähnlich `cvs`). Ist der Server korrekt eingerichtet (mit entsprechendem Repository), kann der Inhalt von jedem Client darauf wie folgt angezeigt werden:

```
svn list http://svn.example.com/pfad/zum/projekt
```

oder

```
svn list svn://svn.example.com/pfad/zum/projekt
```

Mit dem Befehl `svn checkout` können Sie ein existierendes Projekt in das aktuelle Verzeichnis abspeichern (engl. *check out*):

```
svn checkout http://svn.example.com/pfad/zum/projekt projektname
```

Mit dem Auschecken erhält man ein neues Unterverzeichnis `projektname/` auf dem Client. In diesem kann man beliebige Änderungen (hinzufügen, kopieren, umbenennen, löschen) durchführen:

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

Jede dieser Befehle ist nicht nur auf Dateien, sondern auch auf Verzeichnisse anwendbar. Des Weiteren kann subversion auch sog. *properties* (Eigenschaften) zu einer Datei oder Verzeichnis festhalten:

```
svn propset license GPL foo.txt
```

Setzt im vorigem Beispiel für die Datei `foo.txt` die Eigenschaft `license` auf den Wert `GPL`. Durch `svn proplist` können Sie Eigenschaften anzeigen:

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Um Ihre Änderungen zu veröffentlichen, das heisst, auf dem Server zurückzuspielen, gibt man ein:

```
svn commit
```

Damit ein anderer Benutzer Ihre Änderungen in seinem Arbeitsverzeichnis eingespielt bekommt, muss er einen Abgleich mit dem Server über folgendes Kommando vornehmen:

```
svn update
```

Im Gegensatz zu CVS kann der Status eines subversion-Arbeitsverzeichnisses *ohne* Zugriff auf das Repository angezeigt werden:

```
svn status
```

Hierbei werden lokale Veränderungen in fünf Spalten angezeigt, die wichtigste Spalte ist die erste:

″	Keine Änderungen
'A'	Objekt wird als Hinzufügung angesetzt
'D'	Objekt wird zur Löschung angesetzt
'M'	Objekt wurde geändert
'C'	Objekt befindet sich im Konflikt
'I'	Objekt wurde ignoriert
'?'	Objekt befindet sich nicht unter Versionskontrolle
'!'	Objekt wird vermisst. Diese Markierung erscheint, wenn es ohne den `svn`-Befehl gelöscht oder verschoben wurde.
' '	Objekt wurde als Datei verwaltet wurde jedoch durch ein Verzeichnis ersetzt oder umgekehrt.

Die zweite Spalte zeigt den Status von Eigenschaften (sog. *properties*) an. Alle weiteren Spalten können im Subversion-Buch (siehe nächster Abschnitt) nachgelesen werden.

Sollten Sie einmal die genauen Parameter eines Befehls nicht mehr wissen, hilft `svn help` weiter:

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

23.5.4 Weiterführende Literatur

Erste Anlaufstelle ist die Homepage von subversion unter `http://subversion.tigris.org`. Ein sehr empfehlenswertes, komplettes englischsprachiges Buch finden Sie nach der Installation des Pakets `subversion-doc` im Verzeichnis `file:///usr/share/doc/packages/subversion/html/book.html`. Dies ist auch online unter `http://svnbook.red-bean.com/svnbook/index.html` erhältlich.

23.6 Einführung in rsync

23.6.1 Einsatzgebiet

rsync bietet sich immer dann an, wenn große Datenmengen regelmäßig übertragen werden müssen, die sich nicht zu stark verändern. Dies ist zum Beispiel bei der Erstellung von Backups häufig der Fall.

Ein weiteres Einsatzgebiet sind sogenannte *staging server*, also Server auf denen zum Beispiel der komplette Verzeichnisbaum eines Webservers bereitgehalten wird, und der regelmäßig auf den eigentlichen Webserver in einer „DMZ“ gespiegelt wird.

23.6.2 Konfiguration und Benutzung

rsync kann man in zwei verschiedenen Modi verwenden. Zum einen kann rsync zum archivieren oder kopieren von Dateien verwendet werden. Hierzu benötigt man auf dem Zielrechner nur eine remote Shell wie zum Beispiel ssh. rsync kann aber auch als `Daemon` verwendet werden, und Verzeichnisse im Netz zur Verfügung stellen.

Die grundlegende Benutzung von rsync erfordert keine besondere Konfiguration. Mit rsync ist es direkt möglich, komplette Verzeichnisse auf einen

anderen Rechner zu spiegeln. Beispielsweise kann man mit folgendem Befehl ein Backup des Heimatverzeichnisses von tux auf einem Backupserver sun anlegen:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Um das Verzeichnis zurück zu spielen, findet folgender Befehl Verwendung:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Bis hierher unterscheidet sich die Benutzung kaum von einem normalen Kopierprogramm wie scp

Damit rsync seine Features voll ausnutzen kann, sollte er im „rsync" Modus betrieben werden. Hierzu wird auf einem der Rechner der Daemon rsyncd gestartet. In diesem Fall muss rsync über die Datei `/etc/rsyncd.conf` konfiguriert werden. Wenn zum Beispiel das Verzeichnis `/srv/ftp` über rsync zugänglich sein soll, kann folgende Konfigurationsdatei verwendet werden:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Danach muss der rsyncd gestartet werden:

```
rcrsyncd start
```

Der rsyncd kann auch beim Bootprozess automatisch gestartet werden. Hierzu muss entweder dieser Dienst in YaST im Runlevel Editor aktiviert werden, oder manuell der Befehl `insserv rsyncd` eingegeben werden.

Alternativ kann rsyncd auch von xinetd gestartet werden. Dies empfiehlt sich aber nur bei Servern auf denen der rsyncd nicht allzu oft verwendet wird. Im obigen Beispiel wird auch ein Logfile über alle Verbindungen angelegt. Dieses wird unter `/var/log/rsyncd.log` abgelegt.

Nun kann der Transfer von einem Client Rechner aus geprüft werden. Die geschieht mit folgenden Befehl:

```
rsync -avz sun::FTP
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/srv/ftp` liegen. Diese Anfrage taucht auch im Logfile unter `/var/log/Ʀsyncd.log` auf. Um den Transfer tatsächlich zu starten, muss noch ein Zielverzeichnis angeben werden. Für das aktuelle Verzeichnis kann das auch der „.“ sein, also zum Beispiel:

```
rsync -avz sun::FTP .
```

Immer dann wenn der rsyncd auf dem Server angesprochen werden soll, müssen zwei Doppelpunkte zwischen dem Servernamen und dem Ziellaufwerk eingegeben werden.

23.6.3 Mögliche Probleme

Per default werden beim Abgleich mit rsync keine Dateien gelöscht. Wenn dies erzwungen werden soll, dann muss zusätzlich die Option `--delete` angegeben werden.

Um sicherzustellen, dass keine neueren Dateien überschrieben werden, kann die Option. `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

23.6.4 Weiterführende Literatur

Wichtige Informationen zu rsync sind in den Manualpages `man rsync` und `man rsyncd.conf` enthalten.

Eine technische Dokumentation zur Vorgehensweise von rsync finden Sie unter `/usr/share/doc/packages/rsync/tech_report.ps`

Aktuelles zu rsync können Sie auf der Web Seite des Projektes unter `http://rsync.samba.org` nachlesen.

23.7 Einführung mailsync

23.7.1 Einsatzgebiet

Mailsync bietet sich im Wesentlichen für drei Aufgaben an:

- Synchronisation lokal gespeicherter E-Mails mit E-Mails, die auf einem Server gespeichert sind.
- Migration von Mailboxen in ein anderes Format bzw. auf einen anderen Server.
- Integritätscheck einer Mailbox bzw. der Suche nach Duplikaten.

23.7.2 Konfiguration und Benutzung

Mailsync unterscheidet zwischen der Mailbox an sich (einem so genannten Store) und der Verknüpfung zwischen zwei Mailboxen (einem so genannten Channel). Die Definitionen der Stores und Channels wird in der Datei `~/.mailsync` abgelegt. Im Folgenden sollen einige Beispiele für Stores vorgestellt werden. Eine einfache Definition sieht zum Beispiel so aus:

```
store saved-messages {
   pat     Mail/saved-messages
   prefix  Mail/
}
```

`Mail/` ist ein Unterverzeichnis im Home des Benutzers, welches Ordner mit E-Mails enthält, unter anderem den Ordner `saved-messages`. Ruft man nun `mailsync` mit dem Befehl `mailsync -m saved-messages` auf, wird ein Index aller Nachrichten in saved-messages aufgelistet. Eine weitere Definition kann wie folgt aussehen:

```
store localdir {
   pat     Mail/*
   prefix  Mail/
}
```

Hier bewirkt der Aufruf von `mailsync -m localdir` das Auflisten aller Nachrichten, die in den Ordnern unter `Mail/` gespeichert sind. Der Aufruf `mailsync localdir` listet dagegen die Ordnernamen.

Die Spezifikation eines Stores auf einem IMAP-Server sieht zum Beispiel so aus:

```
store imapinbox {
   server  {mail.uni-hannover.de/user=gulliver}
   ref     {mail.uni-hannover.de}
   pat     INBOX
}
```

Im obigen Fall wird nur der Hauptordner auf dem IMAP-Server adressiert, ein Store für die Unterordner sieht dagegen wie folgt aus:

```
store imapdir {
   server  {mail.uni-hannover.de/user=gulliver}
   ref     {mail.uni-hannover.de}
   pat     INBOX.*
   prefix  INBOX.
}
```

Unterstützt der IMAP-Server verschlüsselte Verbindungen, sollte man die Server-Spezifikation wie folgt abändern:

```
server {mail.uni-hannover.de/ssl/user=gulliver}
```

bzw. (falls das Server-Zertifikat nicht bekannt ist) in

```
server {mail.uni-hannover.de/ssl/novalidate-cert/user=gulliver}
```

Nun sollen die Ordner unter `Mail/` mit den Unterverzeichnissen auf dem IMAP-Server verbunden werden:

```
channel Ordner localdir imapdir {
   msinfo .mailsync.info
}
```

Dabei wird sich Mailsync in der mit `msinfo` angebenen Datei merken, welche Nachrichten schon synchronisiert wurden. Ein Aufruf von `mailsync Ordner` bewirkt nun Folgendes:

- Auf beiden Seiten wird das Mailbox-Muster (pat) expandiert.
- Von den dabei entstehenden Ordnernamen wird jeweils das Präfix (prefix) entfernt.
- Die Ordner werden paarweise synchronisiert (bzw. angelegt, falls noch nicht vorhanden).

Ein Ordner `INBOX.sent-mail` auf dem IMAP-Server wird also mit dem lokalen Ordner `Mail/sent-mail` synchronisiert (obige Definitionen vorausgesetzt). Dabei wird die Synchronisation zwischen den einzelnen Ordnern folgendermaßen durchgeführt:

- Existiert eine Nachricht schon auf beiden Seiten, passiert gar nichts.
- Fehlt die Nachricht auf einer Seite und ist neu (d. h. nicht in der msinfo-Datei protokolliert) wird sie dorthin übertragen.
- Existiert die Nachricht nur auf einer Seite und ist alt (d. h. bereits in der msinfo-Datei protokolliert), wird sie dort gelöscht (da sie hoffentlich auf der anderen Seite existiert hatte und dort gelöscht wurde).

Um im voraus ein Bild davon zu erhalten, welche Nachrichten bei einer Synchronisation übertragen und welche gelöscht werden, ruft man Mailsync mit einem Channel *und* einem Store gleichzeitig auf: `mailsync Ordner localdir`.

Dadurch erhält man eine Liste aller Nachrichten, die lokal neu sind, als auch eine Liste aller Nachrichten, die bei einer Synchronisation auf der IMAP-Seite gelöscht werden würden!

Spiegelbildlich erhält man mit `mailsync Ordner imapdir` eine Liste aller Nachrichten, die auf der IMAP-Seite neu sind, als auch eine Liste aller Nachrichten, die bei einer Synchronisation lokal gelöscht werden würden.

23.7.3 Mögliche Probleme

Im Fall eines Datenverlustes ist es das sicherste Vorgehen, die zugehörige Channel-Protokolldatei msinfo zu löschen. Dadurch gelten alle Nachrichten, die nur auf jeweils einer Seite existieren, als neu und werden beim nächsten Sync übertragen.

Es werden nur solche Nachrichten in die Synchronisation einbezogen, die eine Message-ID tragen. Nachrichten, in denen diese fehlt, werden schlichtweg ignoriert, das heisst weder übertragen noch gelöscht. Das Fehlen einer Message-ID kommt in der Regel durch fehlerhafte Programme im Prozess der Mailzustellung oder -erzeugung zustande.

Auf bestimmten IMAP-Servern wird der Hauptordner mittels `INBOX`, Unterordner mittels eines beliebigen Namen angesprochen (im Gegensatz zu INBOX und INBOX.name). Dadurch ist es bei solchen IMAP-Server nicht möglich, ein Muster ausschließlich für die Unterordner zu spezifizieren.

Die von Mailsync benutzen Mailbox-Treiber (c-client), setzen nach erfolgreicher Übertragung der Nachrichten auf einen IMAP-Server ein spezielles Status-Flag, wodurch es manchen E-Mail-Programmen, wie zum Beispiel mutt, nicht möglich ist, die Nachrichten als neu zu erkennen. Das Setzen dieses spezielles Status-Flags lässt sich in Mailsync mit der Option `-n` unterbinden.

23.7.4 Weiterführende Literatur

Das im Paket mailsync enthaltene `README` unter `/usr/share/doc/packages/mailsync/` enthält weitere Informationen und Hinweise. Von besonderem Interesse ist in diesem Zusammenhang auch das RFC 2076 "Common Internet Message Headers".

Heterogene Netzwerke

Linux kann nicht nur mit anderen Linux-Rechnern, sondern auch mit Windows- und Macintosh-Rechnern kommunizieren. Dieses Kapitel zeigt Ihnen, worauf Sie dabei achten müssen und wie Sie entsprechende heterogene Netzwerke konfigurieren können.

24.1 Samba 634
24.2 Netatalk 646

24.1 Samba

24.1.1 Einführung in Samba

Mit dem Programmpaket Samba kann ein Unix-Rechner zu einem File- und Printserver für DOS-, Windows- und OS/2 Rechner ausgebaut werden. Das Samba-Projekt wird vom Samba Team betreut und wurde ursprünglich von dem Australier Andrew Tridgell entwickelt.

Samba ist inzwischen ein sehr umfassendes Produkt, so dass wir an dieser Stelle lediglich einen Einblick in seine Funktionalität liefern können. Jedoch kommt die Software mit umfassender digitaler Dokumentation. Diese besteht einerseits aus Handbuchseiten — zwecks Umfang rufen Sie bitte `apropos samba` auf der Kommandozeile auf — und andererseits aus Dokumenten und Beispielen, die Sie bei installiertem Samba auf Ihrem System unter `/usr/share/doc/packages/samba` finden. Dort finden Sie im Unterverzeichnis `examples` auch die kommentierte Beispielkonfiguration `smb.conf.SuSE`.

Beginnend mit SUSE LINUX Version 9.1 steht Ihnen das Paket `samba` in der Version 3 zur Verfügung. Einige wichtige Neuerungen dieses Paketes sind:

- Active Directory support.
- Unicode Support wurde stark verbessert.
- Die internen Authentifizierungsmechanismen wurden komplett überarbeitet.
- Verbesserte Unterstützung für das Windows 200x/XP Drucksystem.
- Konfiguration als Mitglieds-Server in Active-Directory-Domänen.
- NT4-Domänenübernahme um von einer NT4 Domäne zu einer Samba Domäne zu migrieren.

Samba benutzt das SMB-Protokoll (Server Message Block), das auf den NetBIOS Diensten aufgesetzt ist. Auf Drängen der Firma IBM gab die Firma Microsoft das Protokoll frei, sodass auch andere Software-Hersteller Anbindungen an ein Microsoft-Domain-Netz finden konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das Protokoll TCP/IP installiert sein. Wir empfehlen die ausschließliche Verwendung von TCP/IP auf den Clients.

Hinweis

Migration nach Samba3

Wenn Sie von Samba 2.x nach Samba 3 migrieren möchten, so sind einige Besonderheiten zu beachten. Diesem Thema wurde in der Samba-HOWTO-Collection ein eigenes Kapitel gewidmet. Nach der Installation des Paketes `samba-doc` finden Sie das HOWTO unter `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Hinweis

NetBIOS

Hinweis

S/390, zSeries: NetBIOS-Unterstützung

IBM S/390 und zSeries unterstützen lediglich SMB über TCP/IP. Eine NetBIOS-Unterstüzung existiert auf diesen Systemen nicht.

Hinweis

NetBIOS ist eine Softwareschnittstelle (API), die zur Rechnerkommunikation entworfen wurde. Dabei wird ein Namensdienst (engl. *name service*) bereitgestellt, der zur gegenseitigen Identifikation der Rechner dient. Für die Namensvergabe gibt es keine zentrale Instanz, die Rechte vergeben oder überprüfen könnte. Jeder Rechner am Netz kann beliebig Namen für sich reservieren, sofern diese noch nicht vergeben sind. Die NetBIOS-Schnittstelle kann auf unterschiedlichen Netzarchitekturen implementiert werden. Eine Implementation erfolgt relativ „dicht“ an der Netzwerkhardware und nennt sich NetBEUI. NetBEUI wird häufig als NetBIOS bezeichnet. Netzwerkprotokolle, mit denen NetBIOS implementiert wurde, sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die NetBIOS-Namen, die auch bei der Implementation von NetBIOS mittels TCP/IP vergeben werden, haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein vollständig eigener Namensraum. Es empfiehlt sich jedoch zwecks vereinfachter Administration, zumindest für die Server NetBIOS-Namen zu vergeben, die ihrem DNS-Hostnamen entsprechen. Für einen Samba-Server ist das die Voreinstellung.

Clients

Alle gängigen Betriebssysteme wie Mac OS X, Windows und OS/2 unterstützen das SMB-Protokoll. Auf den Rechnern muss das TCP/IP Protokoll installiert sein. Für die verschiedenen UNIX Versionen stellt Samba einen Client zur Verfügung. Für Linux gibt es zudem ein Dateisystem-Kernel-Modul für SMB, dass das Einbinden von SMB-Ressourcen auf Linux-Systemebene gestattet.

SMB-Server stellen den Clients Plattenplatz in Form von Freigaben, so genannten „Shares“ zur Verfügung. Dabei umfasst ein Share ein Verzeichnis mit allen Unterverzeichnissen auf dem Server. Es wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Dabei kann der Sharename frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem exportierten Drucker ein Name zugeordnet, unter dem Clients darauf zugreifen können.

24.1.2 Installation und Konfiguration des Servers

Wenn Sie Samba als Server einsetzen möchten, installieren Sie das Paket `samba`. Manuell werden die für Samba erforderlichen Dienste mit `rcnmb start & & rcsmb start` gestartet und mit `rcsmb stop & & rcnmb stop` beendet.

Die zentrale Konfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Die Datei kann man logisch in zwei Bereiche trennen. In der so genannten `[global]`-Section werden zentrale und übergreifende Einstellungen vorgenommen. Im zweiten Teilbereich, den `[share]`-Sections, werden die einzelnen Datei- und Drucker-Freigaben definiert. Mittels dieses Vorgehens können Details der Freigaben unterschiedlich oder in der `[global]`-Sektion übergreifend gesetzt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei.

global-Section anhand der Beispielkonfiguration

Die folgenden Parameter der `global`-Section sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server im Windows-Netz von anderen Systemen per SMB erreichbar ist.

workgroup = TUX-NET Der Samba-Server wird mittels dieser Zeile einer Arbeitsgruppe zugeordnet. Zum Betrieb passen Sie `TUX-NET` an die bei Ihnen vorhandene Arbeitsgruppe an oder konfigurieren Ihren Clients auf den hier gewählten Wert. Ihr Samba-Server erscheint

bei dieser Konfiguration mit seinem DNS-Namen in der gewählten Arbeitsgruppe, insoweit der Name noch nicht vergeben ist.

Sollte der Name bereits vergeben sein, kann er mit `netbios name = MEINNAME` abweichend vom DNS-Namen gesetzt werden. Details zu diesem Parameter sind per `man smb.conf` verfügbar.

os level = 2 Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (engl. *Local Master Browser*) für seine Arbeitsgruppe zu werden. Der im Beispiel genutzte Wert ist bewusst niedrig gewählt, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Details zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs/` der Paketdokumentation.

Wird nicht bereits ein SMB-Server — zum Beispiel Windows NT, 2000 Server — betrieben und soll der Samba-Server im lokalen Netz die Namen der verfügbaren Systeme vorhalten, so erhöhen Sie den `os level` auf einen höheren Wert (zum Beispiel 65), um die Wahl zum LMB zu gewinnen.

Bei der Änderung dieses Wertes sollten Sie besonders vorsichtig sein, da Sie den Betrieb eines vorhandenen Windows-Netzes stören können. Reden Sie mit Ihrem Administrator, testen Sie Änderungen zuerst in einem isolierten Netz oder zu unkritischen Zeiten.

wins support und wins server Wenn Sie den Samba-Server in ein vorhandenes Windows-Netz integrieren möchten, in dem bereits ein WINS-Server betrieben wird, benötigen Sie den Parameter `wins server`. Dieser Parameter muss auf die IP-Adresse Ihres WINS-servers gesetzt werden.

Wenn Ihre Windows-Systeme in getrennten Sub-Netzen betrieben werden, und sich gegenseitig sehen sollen, benötigen Sie einen WINS-Server. Um den Samba-Server zum WINS-Server zu machen, benötigen Sie die Option `wins support = Yes`. Achten Sie unbedingt darauf, dass Sie diesen Parameter ausschließlich bei einem Samba-Server aktivieren.

In Ihrer smb.conf dürfen nie beide Optionen, `wins server` und `wins support`, zusammen aktiviert werden.

Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnisse der Nutzer, `homes` für SMB-Clients freigegeben.

[cdrom] Um die versehentliche Freigabe einer CD-ROM zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe mittels Kommentarzeichen – hier Semikolons – deaktiviert. Wollen Sie das CD-ROM-Laufwerk per Samba freigeben, entfernen Sie bitte die Semikolons in der ersten Spalte.

Beispiel 24.1: *CD-ROM-Freigabe*

```
;[cdrom]
;      comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` **und** `comment` Der Eintrag `[cdrom]` ist der den SMB-Clients sichtbare Freigabename. Mittels `comment` kann den Clients eine aussagekräftigere Bezeichnung der Freigabe mitgeteilt werden.

`path = /media/cdrom` Mit `path` wird das Verzeichnis `media/cdrom/` exportiert.

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Nutzer verfügbar. Soll die Freigabe für jedermann bereitgestellt werden, ermöglicht man dies mit der zusätzlichen Zeile `guest ok = Yes`. Aufgrund der sich daraus ergebenden Lesemöglichkeit für jedermann, sollte man mit dieser Einstellung sehr vorsichtig umgehen und sie allein auf ausgesuchte Freigaben anwenden. Für die Verwendung in der `[global]`-Section gilt besondere Vorsicht.

[homes] Eine besondere Stellung nimmt die so genannte `[homes]`-Freigabe ein. Hat der Benutzer auf dem Linux-File-Server einen gültigen Account und ein eigenes Home-Verzeichnis, so kann sich sein Client bei gültiger Nutzerkennung und Passwort mit diesem verbinden.

Beispiel 24.2: *Freigabe homes*

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = No
        read only = No
        create mask = 0640
        directory mask = 0750
```

`[homes]` Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des sich verbindenden Nutzers existiert, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe erzeugt. Dabei ist der Freigabename identisch mit dem Nutzernamen.

`valid users = %S` Das `%S` wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabenamen ersetzt. Da dies bei der `[homes]`-Freigabe immer mit dem Nutzernamen identisch ist, werden die zulässigen Nutzer auf den Eigentümer des Nutzerverzeichnisses beschränkt. Dies ist eine Möglichkeit, um den Zugriff allein dem Eigentümer zu gestatten.

`browseable = No` Durch diese Einstellung ist die `[homes]`-Freigabe nicht in der Liste der Freigaben sichtbar.

`read only = No` Samba verbietet in der Voreinstellung den Schreibzugriff auf exportierte Freigaben, `read only = Yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss man den Wert `read only = No` setzten. Dies ist gleichbedeutend mit `writeable = Yes`.

`create mask = 0640` Nicht auf MS Windows NT basierende Systeme kennen das Konzept der Unix-Zugriffsrechte nicht. Daher können sie bei der Erstellung von Dateien auch nicht angeben, mit welchen Zugriffsrechten dies zu geschehen hat. Der Parameter `create mask` legt fest, mit welchen Zugriffsrechten Dateien angelegt werden. Dieses gilt nur für schreibbare Shares. Konkret wird hier dem Eigentümer das Lesen und Schreiben und Mitgliedern der primären Gruppe des Eigentümers das Lesen erlaubt. Bitte beachten Sie, dass `valid users = %S` selbst dann den lesenden Zugriff verhindert, wenn die Gruppe leseberechtigt ist. Entsprechend muss bei gewünschtem Lese- oder Schreibzugriff für die Gruppe die Zeile `valid users = %S` deaktiviert werden.

Security Level

Das SMB-Protokoll kommt aus der DOS-/Windows-Welt und berücksichtigt die Sicherheitsproblematik direkt. Jeder Zugang zu einem Share kann mit einem Passwort geschützt werden. SMB kennt drei verschiedene Möglichkeiten der Berechtigungsprüfung.

Share Level Security (security = share):
Bei der Share Level Security wird einem Share ein Passwort fest zugeordnet. Jeder, der dieses Passwort kennt, hat Zugriff auf das Share.

User Level Security (security = user):
Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich bei einem Server mit einem Passwort anmelden. Nach der Authentifizierung kann der Server dann, abhängig vom Benutzernamen, Zugang zu den einzelnen, exportierten Shares gewähren.

Server Level Security (security = server):
Samba behauptet gegenüber den Clients, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Diese Einstellung erwartet einen weiteren Parameter (`password server =`).

Die Unterscheidung zwischen Share, User und Server Level Security gilt für den gesamten Server. Es ist nicht möglich, einzelne Shares einer Server-Konfiguration per Share Level Security und andere per User Level Security zu exportieren. Jedoch können Sie auf einem System pro konfigurierter IP-Adresse einen eigenen Samba-Server betreiben.

Weitere Infos zu diesem Thema finden Sie in der Samba-HOWTO-Collection. Für mehrere Server auf einem System beachten Sie bitte die Parameter `interfaces` und `bind interfaces only`.

Hinweis

Für die einfache Administration des Samba-Servers gibt es noch das Programm swat. Es stellt ein einfaches Webinterface zur Verfügung, mit dem Sie bequem den Samba-Server konfigurieren können. Rufen Sie in einem Webbrowser `http://localhost:901` auf und loggen Sie sich als Benutzer root ein. Bitte beachten Sie, dass swat auch in den Dateien `/etc/xinetd.d/samba` und `/etc/services` aktiviert ist. Hierzu müssen Sie in `/etc/xinetd.d/samba` den Parameter `disable` auf `no`ändern. Weitere Informationen zu swat finden Sie in der Manualpage von swat.

Hinweis

24.1.3 Samba als Anmelde-Server

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich die Benutzer nur mit gültigem Account und Passwort anmelden dürfen. Dies kann mit Hilfe eines Samba-Servers realisiert werden. In einem Windows basierten Netzwerk übernimmt ein Windows-NT-Server diese Aufgabe, dieser ist als so genannter Primary Domain Controller (PDC) konfiguriert. Es müssen Einträge in die `[global]`-Section der `smb.conf` vorgenommen werden wie in Beispiel 24.3.

Beispiel 24.3: *Global-Section in smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Werden verschlüsselte Passwörter zur Verifizierung genutzt - dies ist Standard mit gepflegten MS Windows 9x Versionen, MS Windows NT 4.0 ab service pack 3 und allen späteren Produkten -, muss der Samba Server damit umgehen können. Der Eintrag `encrypt passwords = yes` in der `[global]`-Section ermöglicht dies und ist bei samba ab Version 3 default. Außerdem müssen die Benutzeraccounts bzw. die Passwörter in eine Windows konforme Verschlüsselungsform gebracht werden. Das geschieht mit dem Befehl `smbpasswd -a name`. Da nach dem Windows NT Domänenkonzept auch die Rechner selbst einen Domänen-Account benötigen, wird dieser mit den folgenden Befehlen angelegt:

Beispiel 24.4: *Anlegen eines Maschinenaccounts*

```
useradd rechnername\$
smbpasswd -a -m rechnername
```

Bei dem Befehl `useradd` wurde ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` selbst hinzu.

In der kommentierten Beispielskonfiguration `/usr/share/doc/packages/samba/examples/smb.conf.SuSE` sind Einstellungen vorgesehen, die diese Arbeiten automatisieren.

Beispiel 24.5: *Automatisiertes Anlegen eines Maschinenaccounts*

```
add machine script = /usr/sbin/useradd -g machines \
                     -c "NT Machine Account" -d \
                     /dev/null -s /bin/false %m\$
```

Damit dieses Skript von Samba richtig ausgeführt werden kann, benötigen Sie noch einen Samba Benutzer mit Administrator Rechten. Fügen Sie hierzu die Gruppe `ntadmin` dem ausgewählten Benutzer hinzu. Danach können Sie alle Benutzer dieser Unix Gruppe zu den „Domain Admins“ mit folgendem Befehl hinzufügen:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Mehr Informationen hierzu finden Sie in der Samba-HOWTO-Collection im Kapitel 12: `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

24.1.4 Installation und Konfiguration mit YaST

Im Menü ‘Start’ (Abbildung 24.1 auf der nächsten Seite) wählen Sie aus, ob Samba überhaupt gestartet wird. Wenn Sie Samba aktivieren, wird der Service auch bei jedem Systemboot neu gestartet.

Im Menü ‘Shares’ (Abbildung 24.2 auf Seite 644) bestimmen Sie, welche Samba-Shares aktiviert sind. Der Knopf ‘Status wechseln’ schaltet zwischen

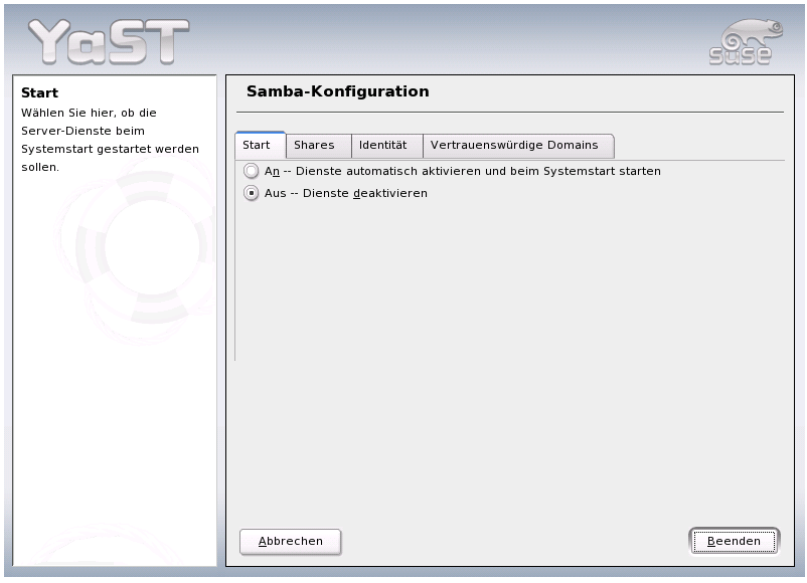

Abbildung 24.1:

den Zuständen ‘aktiv’ und ‘inaktiv’ hin und her. Neue Shares fügen Sie mit ‘Hinzufügen’ hinzu.

Im Menü ‘Identität’ (Abbildung 24.3 auf Seite 645) legen Sie fest, zu welcher Domain der Rechner gehört (‘Grundeinstellungen’) und ob ein alternativer Rechnername im Netz verwendet werden soll (‘NetBIOS Name’). Weiterhin bestimmen Sie, ob der Rechner ein WINS-Server sein soll und, wenn nicht, welcher die IP-Adresse des WINS-Servers ist. Wenn Sie an dieser Stelle ein Stern (*) eintragen, findet YaST den WINS-Server selbständig.

Im Menü ‘Vertrauenswürdige Domains’ (Abbildung 24.4 auf Seite 646) legen Sie fest, welchen domains der Rechner vertrauen soll. Dies bedeutet, das Sie die entsprechenden Einstellungen derjenigen domain, der Sie vertrauen, mit übernehmen.

24.1.5 Installation der Clients

Clients können den Samba-Server nur über TCP/IP erreichen. NetBEUI oder NetBIOS über IPX sind mit Samba nicht verwendbar.

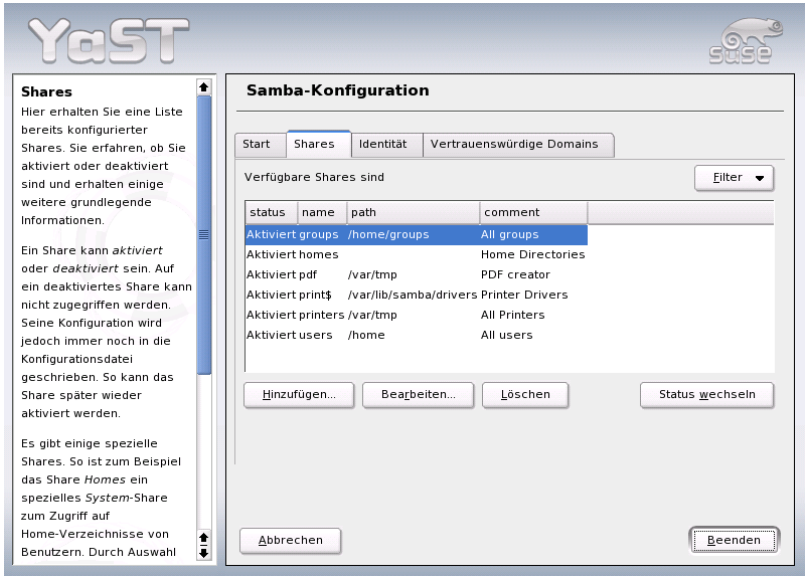

Abbildung 24.2: *Samba Konfiguration -- Shares*

Windows 9x/ME

Windows 9x/ME bringt die Unterstützung für TCP/IP bereits mit. Wie bei Windows for Workgroups wird sie jedoch in der Standardinstallation nicht mitinstalliert. Um TCP/IP nachzuinstallieren, wählt man im Netzwerk-Applet der Systemsteuerung 'Hinzufügen...' unter 'Protokolle' TCP/IP von Microsoft. Nach einem Neustart des Windows-Rechners können Sie den Samba-Server durch Doppelklick auf das Desktop-Symbol für die Netzwerkumgebung finden.

Hinweis

Um einen Drucker auf dem Samba-Server zu nutzen, sollte man den allgemeinen oder den Apple PostScript-Druckertreiber von der jeweiligen Windows-Version installieren; am besten verbindet man dann mit der Linux Drucker-Queue, die PostScript als Input Format akzeptiert.

Hinweis

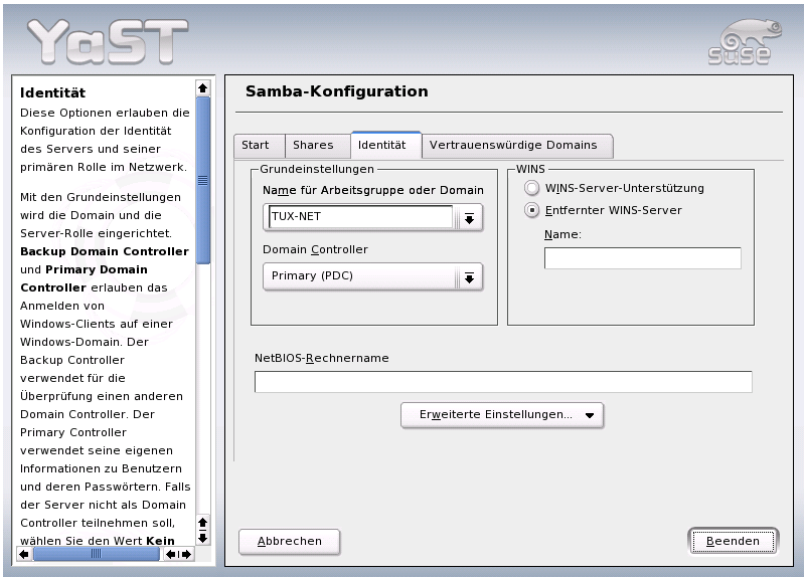

Abbildung 24.3: *Samba Konfiguration -- Identität*

24.1.6 Optimierung

Eine Möglichkeit der Optimierung bietet `socket options`. Die Voreinstellung in der mitgelieferten Beispielkonfiguration orientiert sich an einem lokalen Ethernet-Netzwerk. Weitere Details finden Sie in der Manualpage von `smb.conf` im Abschnitt `socket options` und der Manualpage von `socket(7)`. Weitere Informationen hierzu sind in der `Samba-HOWTO-Collection` im Kapitel `Samba performance tuning` enthalten.

Die Standardkonfiguration in `/etc/samba/smb.conf` versucht sinnvolle Werte vorzuschlagen und orientiert sich dabei an Voreinstellungen des Samba-Teams. Eine fertige Konfiguration ist jedoch insbesondere hinsichtlich der Netzwerkkonfiguration und des Arbeitsgruppennamens nicht möglich. In der kommentierten Beispielkonfiguration `examples/smb.conf.SuSE` finden Sie zahlreiche weiterführenden Hinweise, die bei der Anpassung an lokale Gegebenheiten hilfreich sind.

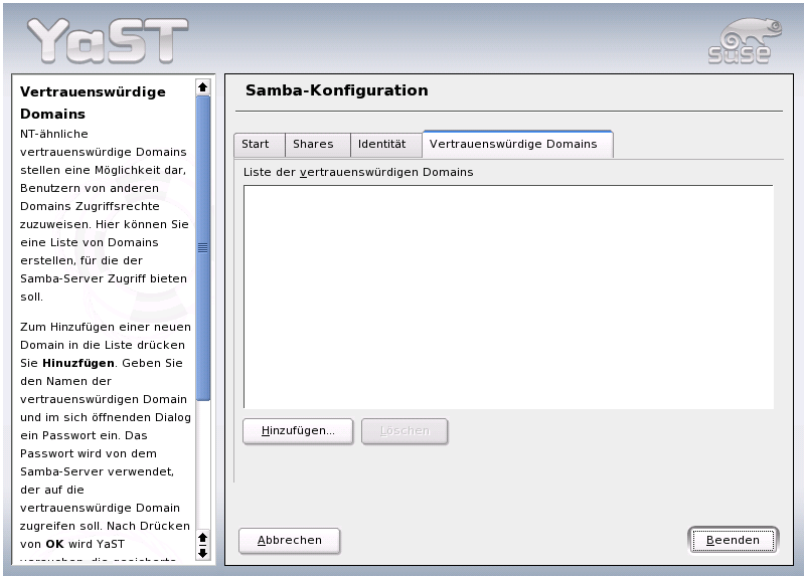

Abbildung 24.4: *Samba Konfiguration -- Vertrauenswürdige Domains*

Hinweis

Das Samba-Team liefert in der `Samba-HOWTO-Collection` einen Abschnitt zur Fehlersuche. In Part V ist außerdem eine Schritt-für-Schritt-Anleitung zur Überprüfung der Konfiguration enthalten.

Hinweis

24.2 Netatalk

Hinweis

S/390, zSeries: Netatalk auf IBM S/390 und zSeries

IBM S/390 und zSeries können das AppleTalk-Protokoll über TCP/IP verwenden. Für reines AppleTalk ist keine Unterstützung vorhanden.

Hinweis

Mit dem `netatalk` können Sie einen leistungsfähigen File- und Druckserver für Mac OS-Clients realisieren. Es ist möglich, von einem Macintosh aus auf Daten des Linux-Rechners zuzugreifen oder auf einem angeschlossenen Drucker zu drucken.

`Netatalk` ist eine Suite von Unix-Programmen, die auf dem im Kernel implementierten DDP (Datagram Delivery Protocol) aufsetzen und die AppleTalk-Protokoll-Familie (ADSP, ATP, ASP, RTMP, NBP, ZIP, AEP und PAP) implementieren.

AppleTalk ist im Prinzip ein Äquivalent zum wesentlich weiter verbreiteten TCP (Transmission Control Protocol). Viele auf TCP/IP aufsetzende Dienste, zum Beispiel zur Auflösung von Hostnamen und Zeitsynchronisation, finden ihre Entsprechung unter AppleTalk. Beispielsweise wird an Stelle von von ping (ICMP ECHO_REQUEST, Internet Control Message Protocol) der Befehl aecho (AEP, AppleTalk Echo Protocol) verwendet.

Folgende drei Daemonen werden normalerweise auf dem Server gestartet:

- Der atalkd („AppleTalk-Netzwerk-Manager“), der dem Programm ip entspricht;
- afpd („AppleTalk Filing Protocol daemon“), der für Macintosh-Clients ein Interface zu Unix-Dateisystemen zur Verfügung stellt;
- papd („Printer Access Protocol daemon“), der Drucker im (AppleTalk-) Netz bereitstellt.

Sie können ohne weiteres – und in heterogenen Netzwerkumgebungen ist dies sehr nützlich – Verzeichnisse auf dem Server nicht nur über `Netatalk`, sondern gleichzeitig über Samba (für Windows-Clients, siehe voriges Kapitel) und über NFS (siehe 21.10 auf Seite 557), exportieren. Datensicherung und die Verwaltung der Nutzerrechte können zentral auf dem Linux-Server erfolgen.

Beachten Sie bitte bei der Verwendung von `Netatalk` folgende Beschränkungen:

- Wegen einer Einschränkung der Macintosh-Clients dürfen die Passwörter der Benutzer auf dem Server maximal 8 Zeichen lang sein.
- Auf Unix-Dateien mit Namen länger als 31 Zeichen können Macintosh-Clients nicht zugreifen.
- Dateinamen dürfen keine Doppelpunkte (`:`) enthalten, weil diese unter Mac OS als Separator in Pfadnamen dienen.

24.2.1 Konfiguration des Fileservers

In der Standardkonfiguration ist `Netatalk` als Fileserver für die auf dem Linux-System eingetragenen Benutzer schon voll funktionsfähig. Um die weitergehenden Features zu nutzen, müssen Sie einige Einstellungen in den Konfigurationsdateien vornehmen. Diese befinden sich im Verzeichnis `/etc/netatalk/`.

Alle Konfigurationsdateien sind reine Textdateien. Text, der hinter einer Raute # steht, wird ignoriert („Kommentare“), leere Zeilen ebenso. Über die Datei `/etc/netatalk/netatalk.conf` werden die verschiedenen Dienste (Drucker, Appletalk Broadcast, Appletalk via TCP/IP, Timeserver) aktiviert:

```
ATALKD_RUN=yes
PAPD_RUN=yes
AFPD_RUN=yes
TIMELORD_RUN=no
```

Netz konfigurieren – atalkd.conf

In `/etc/netatalk/atalkd.conf` legt man fest, über welche Interfaces die Dienste angeboten werden. Meist ist dies `eth0`, und es genügt, wenn hier wie in der Beispieldatei als einziger Wert `eth0` eingetragen ist. Tragen Sie weitere Interfaces ein, wenn Sie zum Beispiel mehrere Netzwerkkarten gleichzeitig verwenden. Wird der Server gestartet, sucht er im Netzwerk nach bereits vorhandenen Zonen und Servern und verändert die entsprechende Zeile, indem er die konfigurierten AppleTalk-Netzwerk-Adressen einträgt. Am Ende der Datei finden Sie dann eine Zeile entsprechend folgender:

```
eth0 -phase 2 -net 0-65534 -addr 65280.57
```

Sollten Sie komplexere Konfigurationen vornehmen wollen, finden Sie in der Konfigurationsdatei Beispiele. Dokumentation über weitere Optionen können Sie außerdem der Manual-Page zum `afpd` entnehmen.

► **S/390, zSeries**
IBM S/390 und zSeries unterstützt nur die Netzwerkkonfiguration über das IP-Protokoll. Das Vorgehen unter AppleTalk ist nicht unterstützt. ◄

Fileserver definieren – afpd.conf

In der Datei `afpd.conf` wird festgelegt, wie Ihr Fileserver auf Mac-OS-Rechnern in der 'Auswahl' erscheint. Wie die anderen Konfigurationsdateien enthält auch diese ausführliche Kommentare, die die vielfältigen Optionen erklären.

Ändern Sie hier nichts, wird einfach der Default-Server gestartet und in der 'Auswahl' mit dem Hostnamen angezeigt. Sie müssen also hier nicht unbedingt etwas eintragen, allerdings ist es auch möglich, Fileserver mit verschiedenen Namen und Optionen zu definieren, um zum Beispiel einen speziellen „Guest Server" anzubieten, auf dem man als „Gast" Dateien ablegen kann:

```
"Guest server" -uamlist uams_guest.so
```

Sie können auch einen Server definieren, der keinen Gastzugang erlaubt, sondern nur für Benutzer zugänglich ist, die auf dem Linux-System existieren:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so
```

Dieses Verhalten wird gesteuert durch die Option `uamlist` gefolgt von einer durch Kommata getrennten Liste der zu verwendenden Authentifizierungsmodule. Default ist, dass alle Verfahren aktiv sind.

Ein AppleShare-Server stellt seine Dienste standardmäßig nicht nur über AppleTalk, sondern auch („encapsulated") über TCP/IP zur Verfügung. Der Default-Port ist 548. Für zusätzliche AppleShare-Server (auf dem gleichen Rechner) müssen Sie, wenn diese ebenfalls auch über TCP laufen sollen, dedizierte Ports zuweisen. Die Bereitstellung des Dienstes über TCP/IP ermöglicht den Zugriff auf den Server auch über nicht AppleTalk-Netze wie zum Beispiel das Internet.

Die Syntax wäre dann zum Beispiel:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so -port 12000
```

Der AppleShare-Server erscheint hier im Netz mit dem Namen `Font Server`, erlaubt keinen Zugriff für Gäste und ist auf den Port 12000 eingestellt. Damit ist er auch über TCP/IP-Router hinweg erreichbar.

Welche (auf dem Server liegenden) Verzeichnisse der jeweilige AppleShare-Server dann als Netz-*Volumes* bereitstellt, wird in der Datei `AppleVolumes.default` definiert (die weiter unten näher erläutert wird). Mit der `-defaultvol` Option können Sie für einen einzelnen AppleShare-Server auch eine andere Datei festlegen, in der abweichende Vorgaben gemacht werden, zum Beispiel (in einer Zeile):

```
"Guest server" -uamlist uams_guest.so -defaultvol \
/etc/netatalk/AppleVolumes.guest
```

Weitere Optionen sind in der Datei `afpd.conf` selbst erklärt.

Verzeichnisse und Zugriffsrechte – AppleVolumes.default

Die Verzeichnisse, die exportiert werden sollen, werden in der Datei `AppleVolumes.default` ausgewählt. Die Zugriffsrechte werden dabei durch die unter Unix üblichen Benutzer- und Gruppen-Rechte festgelegt.

Hinweis

Hier hat sich die Syntax teilweise geändert. Bitte berücksichtigen Sie dies, wenn Sie von einer älteren Version updaten; zum Beispiel heißt es statt `access=` jetzt `allow:` (ein charakteristisches Symptom wäre, wenn Sie auf den Mac-Clients unter AppleTalk statt der Laufwerksbezeichnung deren Optionen angezeigt bekommen.) Da bei einem Update die neuen Dateien mit der Endung `.rpmnew` angelegt werden, kann es sein, dass Ihre alten Einstellungen unter Umständen wegen der geänderten Syntax nicht mehr funktionieren.
Wir empfehlen Ihnen, ein Backup von Ihren Konfigurationsdateien zu machen, aus diesen Ihre alten Einstellungen in die neuen Dateien zu übernehmen und diese dann umzubenennen. So profitieren Sie auch von den aktuellen ausführlichen Kommentaren, die zur Erklärung der diversen Optionen in den Konfigurationsdateien enthalten sind.

Hinweis

Neben `AppleVolumes.default` können zusätzliche Dateien angelegt werden, zum Beispiel `AppleVolumes.guest`, die von bestimmten Servern benutzt werden (indem in der Datei `afpd.conf` die `-defaultvol`-Option benutzt wird – siehe voriger Abschnitt).

Die Syntax ist denkbar einfach:

```
/usr/local/psfonts "PostScript Fonts"
```

bedeutet, dass das in dem Rootverzeichnis liegende Linux-Verzeichnis `/usr/local/psfonts/` als AppleShare-Volume mit dem Namen „PostScript Fonts“ freigegeben wird.

Optionen werden, durch Leerzeichen getrennt, an die Zeile angehängt. Eine sehr nützliche Option ist die Zugriffsbeschränkung:

```
/usr/local/psfonts "PostScript Fonts" allow:User1,@gruppe0
```

was den Zugriff auf das Volume „PostScript Fonts“ auf den Benutzer `User1` und alle Mitglieder der Gruppe `gruppe0` beschränkt. Diese müssen natürlich dem Server bekannt sein. Entsprechend können Sie mit `deny:User2` auch explizit Nutzer ausschließen.

Bitte berücksichtigen Sie, dass diese Einschränkungen für den Zugriff über AppleTalk gelten und nichts mit den Rechten zu tun haben, die der User hat, wenn er sich auf dem Server selber einloggen kann.

`Netatalk` legt zur Abbildung der Mac-OS-typischen Ressource-Fork von Dateien im Linux-Dateisystem `.AppleDouble`-Verzeichnisse an. Mit der Option `noadouble` können Sie bestimmen, dass diese Verzeichnisse erst dann angelegt werden, wenn sie tatsächlich benötigt werden. Syntax:

```
/usr/local/guests "Guests" options:noadouble
```

Weitere Optionen und Möglichkeiten entnehmen Sie bitte den Erklärungen in der Datei selbst.

Übrigens: In dieser Konfigurationsdatei finden Sie ebenfalls eine kleine unschuldige Tilde (`'~'`). Diese Tilde steht für das Homeverzeichnis eines jeden Benutzers auf dem Server. Dadurch kann jedem Benutzer automatisch sein Homeverzeichnis bereitgestellt werden, ohne dass jedes einzelne hier explizit angegeben werden müsste. Die installierte Beispieldatei enthält bereits eine Tilde, weshalb `Netatalk` standardmäßig die Homeverzeichnisse bereitstellt, wenn Sie an dieser Datei nichts ändern.

Der afpd sucht außerdem im Homeverzeichnis eines angemeldeten Benutzers nach einer Datei `Applevolumes` oder `.Applevolumes`. Einträge in dieser Datei ergänzen die Einträge in den Serverdateien

`AppleVolumes.system` und `AppleVolumes.default`, um weitere individuelle type/creator-Zuordnungen zu ermöglichen und auf Dateisysteme zuzugreifen. Diese Einträge sind Ergänzungen und ermöglichen keine Zugriffe, die nicht von Serverseite für diesen Benutzer erlaubt sind.

Die Datei `netatalk.pamd` dient der Authentifizierung über PAM (Pluggable Authentication Modules), was in unserem Rahmen hier ohne Bedeutung ist.

Dateizuordnungen – AppleVolumes.system

In der Datei `AppleVolumes.System` legen Sie fest, welche (Mac-OS-typischen) Type- und Creator-Zuordnungen zu bestimmten Dateiendungen erfolgen soll. Eine ganze Reihe von Standardwerten sind schon vorgegeben. Wenn eine Datei mit einem generischen weißen Icon angezeigt wird, ist in diesem Fall noch kein Eintrag vorhanden. Sollten Sie Probleme haben, eine Textdatei eines anderen Systems unter Mac OS korrekt öffnen zu können, bzw. das umgekehrte Problem, kontrollieren Sie dort die Einträge.

24.2.2 Konfiguration des Druckservers

Über die Datei `papd.conf` konfigurierbar wird ein Laserwriter-Dienst zur Verfügung gestellt. Der Drucker `lpd` muss lokal schon funktionieren (siehe Kapitel 13 auf Seite 323). Wenn Sie mit dem Kommando `lpr datei.txt` lokal drucken können, ist der erste Schritt erfolgreich getan.

Sie müssen in `papd.conf` nichts eingeben, wenn unter Linux ein lokaler Drucker eingerichtet ist, da ohne weitere Angaben Druckaufträge einfach an den Druck-Daemon lpd weitergegeben werden. Der Drucker meldet sich im AppleTalk-Netz als Laserwriter. Sie können aber auch bestimmte Drucker wie folgt eintragen:

```
Drucker_Empfang:pr=lp:pd=/etc/netatalk/kyocera.ppd
```

Dies lässt den Drucker mit dem Namen `Drucker_Empfang` in der Auswahl erscheinen. Die entsprechende Druckerbeschreibungsdatei gibt es gewöhnlich beim Hersteller. Ansonsten nehmen Sie einfach die Datei `Laserwriter` aus dem Ordner `Systemerweiterungen/`; allerdings können Sie dann meist nicht alle Features benutzen.

24.2.3 Starten des Servers

Der Server wird per `Init-Skript` beim Systemstart gestartet oder per Hand mit: `rcatalk start`. Das Init-Skript befindet sich in `/etc/init.d/atalk`. Den Start erledigt das Startskript im Hintergrund; es dauert ca. eine Minute, bis die AppleTalk-Interfaces konfiguriert und erreichbar sind. Sie können mit einer Statusabfrage sehen, ob es soweit ist (erkennbar daran, dass dreimal `OK` ausgegeben wird):

```
rcatalk status

Checking for service atalk:OKOKOK
```

Gehen Sie nun an einen Mac, der unter Mac OS läuft. Kontrollieren Sie, dass AppleTalk aktiviert ist, wählen Sie 'Filesharing', doppelklicken Sie 'Appleshare'; in dem Fenster sollten Sie nun den Namen Ihres Servers sehen. Doppelklicken Sie ihn und melden sie sich an. Wählen Sie das Laufwerk und – voilà – hier ist Ihr Netzlaufwerk unter Mac OS.

Mit Servern, die nur über TCP und nicht über DDP laufen, können Sie sich verbinden, indem Sie in der 'Auswahl' auf 'Server IP-Adresse' klicken und die entsprechende IP-Adresse, gegebenenfalls gefolgt von einem Doppelpunkt und der Portnummer, eingeben.

24.2.4 Weiterführende Informationen

Um alle Möglichkeiten, die das `netatalk` bietet, voll auszuschöpfen, empfiehlt es sich, in den entsprechenden Manual-Pages zu stöbern. Diese finden Sie mit dem Befehl: `rpm -qd netatalk` Noch ein Hinweis: Die Datei `/etc/netatalk/netatalk.conf` wird in unserer Version von netatalk nicht verwendet, Sie können sie einfach ignorieren. Hilfreiche URLs:

- `http://netatalk.sourceforge.net/`
- `http://www.umich.edu/~rsug/netatalk/`
- `http://www.anders.com/projects/netatalk/`

Internet

Das Internet hat sich als Kommunikationsplatform weltweit durchgesetzt. Linux als Netzwerkbetriebssystem kann vielfältige Aufgaben sowohl als Client als auch als Server in diesem Netz wahrnehmen. In diesem Kapitel sollen einige interessante Themen hierzu beschrieben werden: der Einwahlhelfer smpppd (SUSE Meta PPP-Daemon), die manuelle Konfiguration eines ADSL-Zuganges, falls es bei der Einrichtung mit YaST Probleme geben sollte, und die Konfiguration des Proxies Squid.

► **S/390, zSeries**
Für IBM S/390 und zSeries ist lediglich der Abschnitt über Squid relevant. smpppd und ADSL werden auf diesen Plattformen nicht unterstützt. ◄

25.1 Der smpppd als Einwahlhelfer 656
25.2 Konfiguration eines ADSL / T-DSL Anschlusses . 658
25.3 Proxy-Server: Squid 659

25.1 Der smpppd als Einwahlhelfer

25.1.1 Programmkomponenten zur Einwahl ins Internet

Die meisten Heimanwender besitzen keine feste Anbindung an das Internet, sondern wählen sich bei Bedarf ein. Die Kontrolle über diese Verbindung hat dabei je nach Einwahlart (ISDN oder DSL) der ipppd oder der pppd. Im Prinzip reicht es, diese Programme korrekt zu starten, um online zu sein.

Sofern man über eine Flatrate verfügt, die bei der Einwahl keine zusätzlichen Kosten verursacht, reicht es tatsächlich aus, wenn man den Daemon entsprechend startet. Oftmals wünscht man sich jedoch, die Einwahl besser kontrollieren zu können, sei es über ein KDE-Applet oder auch über ein Kommandozeileninterface. Hinzu kommt, dass das Internet-Gateway oft nicht der eigentliche Arbeitsrechner ist, so dass man die Einwahl in einem per Netz erreichbaren Rechner steuern möchte.

An dieser Stelle kommt der smpppd (SUSE Meta PPP-Daemon) ins Spiel. Er stellt Hilfsprogrammen eine einheitliche Schnittstelle zur Verfügung, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils nötigen pppd oder ipppd, und steuert dessen Einwahlverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung, und übermittelt Informationen über den aktuellen Zustand der Verbindung. Da der smpppd auch über das Netz steuerbar ist, eignet er sich gut, die Einwahl ins Internet von einer Workstation im privaten Subnetz aus zu steuern.

25.1.2 Die Konfiguration des smpppd

Die Konfiguration der Verbindungen, die der smpppd zur Verfügung stellt, wird automatisch durch YaST vorgenommen. Die eigentlichen Einwahlprogramme kinternet und cinternet werden ebenfalls vorkonfiguriert. Handarbeit ist dann gefragt, wenn Sie weitere Features des smpppd, etwa eine remote Bedienung, einrichten möchten.

Die Konfigurationsdatei des smpppd liegt unter `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine remote Bedienung möglich ist. Die interessantesten Optionen dieser Konfigurationsdatei sind:

open-inet-socket = `<yes|no>` Wenn eine Steuerung des smpppd über das Netzwerk gewünscht ist, muss diese Option auf `yes` gesetzt werden. Der Port, auf dem der smpppd dann hört, ist `3185`. Wenn

dieser Parameter auf `yes` gesetzt ist, sollten Sie auch die Parameter `bind-address`, `host-range` und `password` sinnvoll setzen.

bind-address = `<ip>` Wenn ein Rechner mehrere IP-Adressen hat, kann damit festgelegt werden, über welche IP-Adresse der smpppd Verbindungen akzeptiert.

host-range = `<min ip> <max ip>`
Der Parameter `host-range` kann verwendet werden, um einen Netzbereich zu definieren. Den Rechnern, deren IP-Adressen in diesem Bereich liegen, wird der Zugang zum smpppd erlaubt. Anders ausgedrückt, es werden alle Rechner abgewiesen, die nicht in diesem Bereich liegen.

password = `<password>` Mit der Vergabe eines Passworts kann eine Einschränkung der Clients auf berechtigte Rechner geschehen. Da dies ein Klartextpasswort ist, sollte man die Sicherheit, die es bietet nicht überbewerten. Wenn kein Passwort vergeben wird, dann sind alle Clients berechtigt, auf den smpppd zuzugreifen.

Weitere Informationen zum smpppd finden Sie in den Manualpages `man smpppd` und `man smpppd.conf`.

25.1.3 kinternet und cinternet im Remote-Einsatz

Die Programme kinternet und cinternet können sowohl lokal verwendet werden als auch einen entfernten smpppd steuern. cinternet ist hierbei auf der Kommandozeile die Entsprechung zum grafischen kinternet. Wenn Sie diese Utilities zum Einsatz mit einem remote smpppd vorbereiten möchten, müssen Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mit Hilfe von kinternet editieren. Diese Datei kennt nur drei Optionen:

server = `<server>` An dieser Stelle können Sie den Rechner spezifizieren, auf dem der smpppd läuft. Wenn dies gleichzeitig das default gateway des Rechners ist, reicht es, `gateway-fallback` auf `yes` zu setzen.

gateway-fallback = `<yes|no>` Wenn weder ein Server spezifiziert wurde noch einer lokal läuft, sprechen Sie einen smpppd auf dem default gateway an. Diese Option ist standardmäßig aktiviert.

password = `<password>` Setzen Sie an dieser Stelle das Passwort ein, das auch für den smpppd ausgewählt wurde.

Sofern der smpppd läuft, können Sie jetzt versuchen, auf den smpppd zuzugreifen. Dazu bietet sich der Befehl `cinternet --verbose --interface-list` an. Sollten Sie an dieser Stelle noch Schwierigkeiten haben, dann lesen Sie bitte die Manualpages `man smpppd-c.conf` und `man cinternet`.

25.2 Konfiguration eines ADSL / T-DSL Anschlusses

25.2.1 Standardkonfiguration

Momentan werden von SuSE Linux DSL-Zugänge unterstützt, die mit dem Point-to-Point-over-Ethernet-Protokoll (PPPoE) arbeiten. Dieses Protokoll wird von allen großen Anbietern benutzt. Sollten Sie sich nicht sicher sein, welches Protokoll Ihr Provider verwendet, gibt dieser sicherlich gerne Auskunft.

Die Pakete `ppp` und `smpppd` müssen installiert werden. Verwenden Sie dazu am besten YaST. Konfigurieren Sie Ihre Netzwerkkarte mit YaST. Verwenden Sie nicht `dhcp`, sondern vergeben Sie eine statische IP Adresse, zum Beispiel `192.168.2.22`.

Die Parameter, die Sie mit dem YaST DSL-Modul bearbeiten, werden in der Datei `/etc/sysconfig/network/providers/provider0/` abgespeichert. Zusätzlich gibt es noch Konfigurationsdateien für den smpppd (SuSE Meta-PPP-Daemon) und seine Frontends kinternet und cinternet. Bitte beachten Sie dazu die Manualpage `man smpppd`.

Starten Sie das Netzwerk ggf. mit dem Befehl `rcnetwork start` und danach den smpppd mit dem Befehl `rcsmpppd start`.

Mit den Befehlen `cinternet --start` und `cinternet --stop` können Sie auf einem System ohne graphischer Oberfläche eine Verbindung herstellen bzw. abbrechen. Auf einer graphischen Benutzeroberfläche können Sie dazu kinternet benutzen. Dieses Programm wird unter KDE automatisch gestartet, falls Sie DSL mit YaST eingerichtet haben. Klicken Sie auf das Zahnrad-Icon in der Buttonleiste. Wählen Sie 'Kommunikation/Internet' → 'Internet Tools' → 'kinternet'. Nun erscheint in der Buttonleiste das Steckersymbol. Ein Klick darauf startet die Verbindung und ein zweiter Klick beendet sie wieder.

25.2.2 DSL Verbindung per Dial-on-Demand

Dial-on-Demand bedeutet, dass die Verbindung automatisch aufgebaut wird, sobald ein User auf das Internet zugreift, zum Beispiel indem er eine Webseite mit einem Browser anwählt oder E-Mails verschickt. Nach einer bestimmten Zeit (Idletime), in der keine Daten gesendet oder empfangen werden, wird die Verbindung wieder getrennt. Da die Einwahl mit PPPoE, dem Protokoll für ADSL, sehr schnell geht, entsteht mitunter der Eindruck, als hätte man eine Standleitung in das Internet.

Dies ist aber nur sinnvoll, wenn Sie eine Flatrate besitzen. Wird Ihr Zugang zeitabhängig abgerechnet, müssen Sie darauf achten, dass kein periodischer Prozess, zum Beispiel ein cronjob, immer wieder eine Verbindung aufbaut. Das könnte Ihre Kosten in die Höhe treiben.

Obwohl mit einer DSL-Flatrate auch eine permanente Einwahl möglich wäre, sprechen doch einige Punkte für eine Verbindung, die nur kurz und nach Bedarf besteht:

- Die meisten Provider trennen die Verbindung nach einer gewissen Zeit.
- Eine permanente Verbindung kann als Ressourcenverschwendung betrachtet werden (zum Beispiel IP-Adressen).
- Vor allem ist es ein enormes Sicherheitsrisiko, permanent online zu sein, da ein Angreifer das System auf Schwachstellen absuchen kann. Ein System, das nur bei Bedarf im Internet erreichbar ist und immer wieder eine andere IP-Adresse hat, ist viel schwieriger zu attackieren.

Dial-on-Demand können Sie mit YaST aktivieren oder Sie richten es manuell ein. Setzen Sie in der Datei `/etc/sysconfig/network/providers/provider0/` den Parameter `DEMAND=` auf `"yes"` und definieren Sie eine Idletime mit der Variable: `IDLETIME="60"`. Damit wird eine unbenutzte Verbindung nach 60 Sekunden beendet.

Zur Einrichtung eines DSL-Gateways für private Netzwerke empfehlen wir folgenden Artikel in unserer Supportdatenbank: `http://portal.suse.de/sdb/de/2002/07/masq80.html`

25.3 Proxy-Server: Squid

Squid ist ein weit verbreiteter Proxy-Cache für Linux/UNIX-Plattformen. Wir werden beschreiben, wie er zu konfigurieren ist, welche Systemanforderungen bestehen, wie das eigene System konfiguriert sein muss, um

transparentes Proxying durchzuführen, wie man Statistiken über die Nutzung des Cache mithilfe von Programmen wie Calamaris und cachemgr erhält oder wie man Web-Inhalte mit squidGuard filtert.

25.3.1 Was ist ein Proxy-Cache?

Squid fungiert als Proxy-Cache. Er leitet Anfragen nach Objekten von Clients (in diesem Fall von Web-Browsern) an den Server weiter. Wenn die angeforderten Objekte von dem Server ankommen, liefert er die Objekte an den Client und behält eine Kopie davon in dem Festplatten-Cache.

Ein Vorteil des Cachings besteht darin, dass mehrere Clients, die dasselbe Objekt anfordern, aus dem Festplatten-Cache bedient werden können. Die Clients erhalten die Daten also wesentlich schneller als aus dem Internet. Dieses Vorgehen spart gleichzeitig Netzwerk-Transfervolumen.

Neben dem eigentlichen Caching bietet Squid ein großes Spektrum an Features: zum Beispiel die Festlegung von Hierarchien für die Proxy-Server zum Verteilen der Systemlast, Aufstellen fester Zugriffsregeln an alle Clients, die auf den Proxy zugreifen wollen, Erteilen oder Verweigern von Zugriffsrechten auf bestimmte Webseiten mit Hilfe anderer Applikationen oder die Ausgabe von Statistiken der meistbesuchten Webseiten und somit zum das Surfverhalten der Benutzer.

Squid ist kein generischer Proxy. Normalerweise vermittelt er nur zwischen HTTP-Verbindungen. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, jedoch keine anderen Internet-Protokolle wie Real Audio, News oder Videokonferenzen. Squid greift auf das UDP-Protokoll nur zur Unterstützung der Kommunikation zwischen verschiedenen Caches zurück. Aus diesem Grund werden auch andere Multimedia-Programme nicht unterstützt.

25.3.2 Informationen zu Proxy-Cache

Squid und Sicherheit

Man kann Squid zusammen mit einer Firewall verwenden, um interne Netzwerke durch den Einsatz eines Proxy-Cache nach außen zu schützen. Die Firewall verweigert mit Ausnahme von Squid allen Clients den Verbindungsaufbau zu externen Diensten. Alle WWW-Verbindungen müssen dann durch den Proxy aufgebaut werden.

Im Falle einer Firewall-Konfiguration mit einer DMZ würde man dort den Proxy einsetzen. Bei einer solchen Konfiguration ist es wichtig, dass alle

Rechner in der DMZ ihre Protokolldateien an Rechner innerhalb des gesicherten Netzwerks senden.

Ein Möglichkeit der Einrichtung eines so genannten „Transparenten“ Proxy wird in Abschnitt 25.3.6 auf Seite 671 behandelt.

Mehrere Caches

Man kann mehrere Proxies so konfigurieren, dass Objekte zwischen ihnen ausgetauscht werden können; so lässt sich die Systemlast reduzieren und die Wahrscheinlichkeit steigern, ein bereits im lokalen Netzwerk vorhandenes Objekt zu finden. Möglich sind auch Cache-Hierarchien, so dass ein Cache in der Lage ist, Objektanfragen an Caches der gleichen Hierarchie weiterzuleiten oder einen übergeordneten Cache zu veranlassen, die Objekte von einem anderen Cache im lokalen Netzwerk oder direkt aus der Quelle herunterzuladen.

Die Wahl der richtigen Topologie für die Cache-Hierarchie ist sehr wichtig, da Netzwerkverkehr insgesamt nicht erhöht werden soll. In einem großen Netzwerk bietet es sich an, für jedes Subnetz einen Proxy-Server zu konfigurieren und diesen dann mit einem übergeordneten Proxy zu verbinden, der wiederum mit dem Proxy-Cache vom ISP verbunden wird.

Die gesamte Kommunikation wird vom ICP (engl. *Internet Cache Protocol*) gesteuert, das auf dem UDP-Protokoll aufgesetzt ist. Der Datenaustausch zwischen Caches geschieht mittels HTTP (engl. *Hyper Text Transmission Protocol*) basierend auf TCP.

Um den besten Server für die gewünschten Objekte zu finden, schickt ein Cache an alle Proxies der gleichen Hierarchie eine ICP-Anfrage. Die Proxies werden mittels ICP-Antworten mit dem Code „HIT“ auf die Anfragen reagieren, falls das Objekt gefunden wurde oder, falls nicht, mit dem Code „MISS“. Im Falle mehrerer HIT-Antworten wird der Proxy-Server einen Server für das Herunterladen bestimmen. Diese Entscheidung wird unter anderem dadurch bestimmt, welcher Cache die schnellste Antwort sendet oder welcher näher ist. Bei einer nicht zufrieden stellenden Antwort wird die Anfrage an den übergeordneten Cache geschickt.

Hinweis

Zur Vermeidung einer mehrfachen Speicherung von Objekten in verschiedenen Caches des Netzwerks werden ebenfalls ICP-Protokolle verwendet, wie zum Beispiel CARP (engl. *Cache Array Routing Protocol*) oder HTCP (engl. *Hyper-Text Cache Protocol*). Je mehr Objekte sich im Netzwerk befinden, desto leichter wird es, das Gesuchte zu finden.

Hinweis

Zwischenspeichern von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es existieren viele dynamisch generierte CGI-Seiten, Zugriffszähler oder verschlüsselte SSL-Dokumente für eine höhere Sicherheit. Aus diesem Grund werden solche Objekte nicht im Cache gehalten: Bei jedem neuen Zugriff hat sich das Objekt bereits wieder verändert.

Für alle anderen im Cache befindlichen Objekte stellt sich jedoch die Frage, wie lange sie dort bleiben sollen. Für diese Entscheidung werden alle Objekte im Cache verschiedenen Stadien zugeordnet.

Durch Header wie `Last modified` („zuletzt geändert“) oder `Expires` („läuft ab“) und dem entsprechenden Datum informieren sich Web- und Proxy-Server über den Status eines Objekts. Es werden auch andere Header verwendet, die zum Beispiel anzeigen, dass ein Objekt nicht zwischengespeichert werden muss.

Objekte im Cache werden normalerweise aufgrund fehlenden Speichers ersetzt, und zwar durch Algorithmen wie LRU (engl. *Last Recently Used*), die zum Ersetzen von Cache-Objekten entwickelt wurden. Das Prinzip besteht im Wesentlichen darin, zuerst die am seltensten gewünschten Objekte zu ersetzen.

25.3.3 Systemanforderungen

Zuerst sollte die maximale Systemlast bestimmt werden. Es ist wichtig, den Systemspitzen besondere Aufmerksamkeit zu schenken, da diese mehr als viermal so hoch wie der Tagesdurchschnitt sein können. Im Zweifelsfall ist es besser, die Systemanforderungen zu überschätzen, da ein am Limit arbeitender Squid zu einem ernsthaften Qualitätsverlust des Dienstes führen kann.

Geordnet nach Wichtigkeit werden in den folgenden Abschnitten die verschiedenen Systemfaktoren aufgezeigt.

Festplatte

Für das Zwischenspeichern spielt Geschwindigkeit eine hohe Rolle. Man sollte sich also um diesen Faktor besonders kümmern. Bei Festplatten ist dieser Parameter als „Zugriffszeit“ in Millisekunden beschrieben. Als Faustregel gilt: Je niedriger dieser Wert, desto besser. Für eine hohe Geschwindigkeit empfiehlt es sich, schnelle Festplatten zu wählen.

Da Squid zumeist kleinere Datenblöcke von der Festplatte zu liest oder abspeichert, ist die Zugriffszeit einer Festplatte wichtiger als der Durchsatz. Gerade hierbei rentieren sich Festplatten mit hohen Drehzahlen, die eine schnelle Positionierung des Lesekopfes ermöglichen. Schnelle SCSI-Festplatten erreichen heute Zugriffszeiten unter 4 Millisekunden.

Eine Möglichkeit, die Geschwindigkeit zu erhöhen, ist der gleichzeitige Einsatz mehrerer Festplatten oder *Striping Raid Arrays*.

Größe des Festplatten-Cache

In einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (das gewünschte Objekt befindet sich bereits dort) sehr gering, da der Cache schnell gefüllt sein wird. In diesem Fall werden die selten gewünschten Objekte durch neue ersetzt. Steht jedoch zum Beispiel 1 GB für den Cache zur Verfügung und die Benutzer benötigen nur 10 MB pro Tag zum Surfen, dann dauert es mehr als hundert Tage, bis der Cache voll ist.

Am leichtesten lässt sich die Größe des Cache durch die maximale Übertragungsrate der Verbindung bestimmen. Mit einer Verbindung von 1 Mbit/s wird die maximale Übertragungsrate bei 125 KB/s liegen. Landet der gesamte Datenverkehr im Cache, kommen innerhalb einer Stunde 450 MB zusammen. Wenn man nun annimmt, dass der gesamte Datenverkehr lediglich während acht Arbeitsstunden erzeugt wird, erreicht man innerhalb eines Tages 3,6 GB. Da die Verbindung normalerweise nicht bis zur Kapazitätsgrenze ausgeschöpft wird, kann man davon ausgehen, dass die gesamte Datenmenge, die der Cache bearbeitet, bei ungefähr 2 GB liegt. In diesem Beispiel werden demnach 2 GB Speicher für Squid benötigt, um die Daten aller aufgerufenen Seiten *eines* Tages im Cache zu halten.

RAM

Der von Squid benötigte Speicher (RAM) ist abhängig von der Anzahl der im Cache zugewiesenen Objekte. Squid speichert Cache-Objektverweise und häufig angeforderte Objekte zusätzlich im Hauptspeicher, damit diese Daten schneller abgefragt werden können. Der Hauptspeicher ist sehr viel schneller als eine Festplatte!

Squid hält auch andere Daten im Speicher, zum Beispiel eine Tabelle mit allen vergebenen IP-Adressen, einen genau festgelegten Domainnamen-Cache, die am häufigsten gewünschten Objekte, Puffer, Zugriffskontrolllisten, etc.

Es ist sehr wichtig, dass ausreichend Speicher für den Squid-Prozess zur Verfügung steht. Sollte er auf Festplatte ausgelagert werden müs-

sen, wird sich die Systemleistung drastisch reduzieren. Für die Cache-Speicherverwaltung kann das Tool cachemgr.cgi verwendet werden. Es wird im Abschnitt 25.3.7 auf Seite 674 erläutert.

CPU

Das Programm Squid benötigt nicht viel CPU. Nur beim Start und während der Überprüfung des Cache-Inhalts ist die Prozessorlast höher. Der Einsatz eines Multiprozessorrechners steigert die Systemleistung nicht. Zur Effektivitätssteigerung ist es besser, schnellere Festplatten zu verwenden oder mehr Speicher hinzuzufügen.

25.3.4 Squid starten

Der Squid auf SUSE LINUX ist bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann. Als Voraussetzung für einen reibungslosen Start sollte das Netzwerk soweit konfiguriert sein, dass mindestens ein Nameserver und sinnvollerweise auch das Internet erreichbar sind. Probleme kann es bereiten, wenn man eine Wählverbindung mit dynamischer DNS-Konfiguration verwendet. In so einem Fall sollte mindestens der Nameserver fest eingetragen sein, da Squid erst gar nicht startet, wenn er in der `/etc/resolv.conf` keinen DNS-Server findet.

Um Squid zu starten, gibt man auf der Kommandozeile (als `root`) den Befehl `rcsquid start` ein. Beim ersten Mal wird zunächst die Verzeichnisstruktur in `/var/squid/cache` angelegt. Dies wird vom Startskript `/etc/init.d/squid` automatisch durchgeführt und kann ein paar Sekunden bis Minuten dauern. Erscheint rechts in grün *done*, wurde Squid erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit von Squid sofort testen, indem man im Browser als Proxy `localhost` und als Port `3128` einträgt.

Um den Zugriff auf Squid und somit das Internet für alle zu ermöglichen, braucht man in der Konfigurationsdatei `/etc/squid/squid.conf` lediglich den Eintrag `http_access deny all` auf `http_access allow all` zu ändern. Allerdings sollte man dabei bedenken, dass man den Squid damit komplett für jedermann öffnet. Von daher sollte man unbedingt ACLs definieren, die den Zugriff auf den Proxy regeln. Dazu mehr im Abschnitt 25.3.5 auf Seite 669.

Hat man Änderungen an der Konfigurationsdatei `/etc/squid/squid.conf` vorgenommen, muss Squid diese neu einzulesen; das geschieht mit dem Kommando: `rcsquid reload`. Alternativ kann man Squid auch komplett neu starten: `rcsquid restart`.

Wichtig ist noch folgendes Kommando: `rcsquid status`. Damit kann man feststellen, ob der Proxy läuft und mit `rcsquid stop` wird Squid beendet. Letzteres kann eine Weile dauern, da Squid bis zu einer halben Minute (Option `shutdown_lifetime` in `/etc/squid/squid.conf`) wartet, bevor die Verbindungen zu den Clients unterbrochen werden und er dann noch seine Daten auf Platte schreiben muss.

Achtung

Beenden von Squid

Beendet man Squid mit `kill` oder `killall`, kann das einen zerstörten Cache zur Folge haben; einen solchen zerstörten Cache muss man löschen, um Squid wieder starten zu können.

Achtung

Beendet sich Squid nach kurzer Zeit, obwohl er anscheinend erfolgreich gestartet wurde, kann das an einem fehlerhaften Nameserver-Eintrag oder einer fehlenden `/etc/resolv.conf` liegen. Den Grund für einen gescheiterten Start protokolliert Squid in der Datei `/var/squid/logs/cache.log` . Soll Squid bereits beim Booten automatisch gestartet werden, muss im Runlevel-Editor von YaST Squid für die gewünschten Runlevel aktiviert werden.

Bei einer Deinstallation von Squid werden weder Cache noch Protokoll-Dateien entfernt. Man muss das Verzeichnis `/var/cache/squid` manuell löschen.

Lokaler DNS-Server

Einen lokalen DNS-Server wie BIND9 aufzusetzen, ist durchaus sinnvoll, auch wenn er keine eigene Domain verwaltet. Er fungiert dann lediglich als „Caching-only DNS“ und kann ohne spezielle Konfiguration DNS-Anfragen über die Root-Nameserver auflösen. Trägt man diesen in der `/etc/resolv.conf` mit der IP-Adresse `127.0.0.1` für `localhost` ein, findet Squid beim Starten immer einen gültigen Nameserver. Es reicht aus, das Paket zu installieren und BIND zu starten. Den Nameserver des Providers

sollte man in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` mit seiner IP-Adresse eintragen. Falls man eine Firewall laufen hat, muss man aber darauf achten, dass die DNS-Anfragen auch durchgelassen werden.

25.3.5 Die Konfigurationsdatei /etc/squid/squid.conf

Alle Einstellungen zum Squid Proxyserver sind in der Datei `/etc/squid/squid.conf` vorzunehmen. Um Squid erstmalig starten zu können, sind darin keine Änderungen erforderlich, der Zugriff von externen Clients ist jedoch zunächst gesperrt. Für `localhost` ist der Proxy freigegeben und als Port wird standardmäßig `3128` verwendet. Die Optionen sind ausführlich und mit vielen Beispielen in der vorinstallierten `/etc/squid/squid.conf` dokumentiert. Annähernd alle Einträge sind am Zeilenanfang durch ein #-Zeichen auskommentiert; am Zeilenende befinden sich die relevanten Spezifikationen. Die angegebenen Werte entsprechen fast immer den voreingestellten Werten, so dass das Entfernen des Kommentarzeichens, ohne den Parameter der Option zu ändern, bis auf wenige Ausnahmen keine Wirkung hat. Es empfiehlt sich, das Beispiel stehen zu lassen und die Option mit dem geänderten Parameter in einer Zeile darunter neu einzufügen. So kann man die voreingestellten Werte und Änderungen problemlos nachvollziehen.

Hinweis

Update von Version 2.4 auf Version 2.5

Nach einem Update von Squid von Version 2.4 auf Version 2.5 muss der Cache des Squid gelöscht werden, da sich das Layout der Verzeichnissstruktur geändert hat.

Hinweis

Hat man ein Update von einer älteren Squid-Version durchgeführt, ist es unbedingt zu empfehlen, die neue `/etc/squid/squid.conf` zu verwenden und nur die Änderungen von der ursprünglichen Datei zu übernehmen. Versucht man die alte `squid.conf` weiter zu verwenden, läuft man Gefahr, dass die Konfiguration nicht mehr funktioniert, da Optionen immer wieder geändert werden und neue hinzukommen.

Allgemeine Konfigurations-Optionen (Auswahl)

http_port 3128 Das ist der Port, auf dem Squid auf Anfragen der Clients lauscht. Voreingestellt ist `3128`, gebräuchlich ist auch `8080`. Es ist möglich, hier mehrere Portnummern, durch Leerzeichen getrennt, anzugeben.

cache_peer <hostname> <type> <proxy-port> <icp-port>
Hier kann man einen übergeordneten Proxy als „Parent“ eintragen, zum Beispiel wenn man den des Providers nutzen will oder muss.

Als <*hostname*> trägt man den Namen bzw. die IP-Adresse des zu verwendenden Proxies und als <*type*> *parent* ein. Für <*proxy-port*> trägt man die Portnummer ein, die der Betreiber des Parent auch zur Verwendung im Browser angibt, meist `8080`. Den <*icp-port*> kann man auf `7` oder `0` setzen, wenn man den ICP-Port des Parent nicht kennt und die Benutzung dieses mit dem Provider nicht vereinbart wurde. Zusätzlich sollte man dann noch *default* und *no-query* nach den Portnummern angeben, um die Verwendung des ICP-Protokolls ganz zu unterbinden. Squid verhält sich dann gegenüber dem Proxy des Providers wie ein normaler Browser.

cache_mem 8 MB Dieser Eintrag gibt an, wie viel Arbeitsspeicher von Squid für das Cachen maximal verwendet wird. Voreingestellt sind `8 MB`.

cache_dir ufs /var/cache/squid 100 16 256
Der Eintrag *cache_dir* gibt das Verzeichnis an, in dem alle Objekte auf Platte abgelegt werden. Die Zahlen dahinter geben den maximal zu verwendenden Plattenplatz in „MB“ und die Anzahl der Verzeichnisse in erster und zweiter Ebene an. Den Parameter *ufs* sollte man unverändert lassen. Voreingestellt sind „100 MB“ Plattenplatz im Verzeichnis `/var/cache/squid` zu belegen und darin 16 Unterverzeichnisse anzulegen, die jeweils wiederum 256 Verzeichnisse enthalten. Bei Angabe des zu verwendenden Plattenplatzes sollte man genügend Reserven lassen, sinnvoll sind Werte zwischen 50 und maximal 80 Prozent des verfügbaren Platzes. Die beiden letzten Zahlen für die Anzahl der Verzeichnisse sollte man nur mit Vorsicht vergrößern, da zu viele Verzeichnisse auch wieder auf Kosten der Performance gehen können. Hat man mehrere Platten, auf die der Cache verteilt werden soll, kann man entsprechend viele *cache_dir*-Zeilen eintragen.

cache_access_log /var/log/squid/access.log
Pfadangabe für Protokoll-Dateien.

cache_log /var/log/squid/cache.log
Pfadangabe für Protokoll-Dateien.

cache_store_log /var/log/squid/store.log
Pfadangabe für Protokoll-Dateien. Diese drei Einträge geben den Pfad zur Protokolldatei von Squid an. Normalerweise wird man daran nichts ändern. Wird der Squid stark beansprucht, kann es sinnvoll sein, den Cache und die Protokoll-Dateien auf verschiedene Platten zu legen.

emulate_httpd_log off Ändert man diesen Eintrag auf *on*, erhält man lesbare Protokoll-Dateien. Allerdings kommen manche Auswerteprogramme damit nicht zurecht.

client_netmask 255.255.255.255 Mit diesem Eintrag kann man die protokollierten IP-Adressen in den Protokoll-Dateien maskieren, um die Identität der Clients zu verbergen. Trägt man hier `255.255.255.0` ein, wird die letzte Stelle der IP-Adresse auf Null gesetzt.

ftp_user Squid@ Hiermit kann man das Passwort setzen, welches Squid für den anonymen FTP-Login verwenden soll. Es kann aber sinnvoll sein, hier eine gültige E-Mail-Adresse in der eigenen Domain anzugeben, da einige FTP-Server diese auf Gültigkeit überprüfen.

cache_mgr webmaster Eine E-Mail-Adresse, an die Squid eine Nachricht schickt, wenn er unerwartet abstürzt. Voreingestellt ist *webmaster*.

logfile_rotate 0 Squid ist in der Lage, die gesicherten Protokoll-Dateien zu rotieren, wenn man `squid -k rotate` aufruft. Die Dateien werden dabei, entsprechend der angegebenen Anzahl, durchnummeriert, und nach Erreichen des angegebenen Wertes wird die jeweils älteste Datei wieder überschrieben. Dieser Wert steht standardmäßig auf `0`, weil das Archivieren und Löschen der Protokoll-Dateien bei SUSE LINUX von einem eigenen Cronjob durchgeführt wird, dessen Konfiguration man in der Datei `/etc/logrotate/squid` findet.

append_domain <domain> Mit *append_domain* kann man angeben, welche Domain automatisch angehängt wird, wenn keine angegeben wurde. Meist wird man hier die eigene Domain eintragen, dann genügt es, im Browser *www* einzugeben, um auf den eigenen Webserver zu gelangen.

forwarded_for on Setzt man diesen Eintrag auf *off*, entfernt Squid die IP-Adresse bzw. den Systemnamen des Clients aus den HTTP-Anfragen.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes
Normalerweise braucht man diese Werte nicht zu verändern. Hat man aber eine Wählleitung, kann es vorkommen, dass das Internet zeitweilig nicht erreichbar ist. Squid merkt sich dann die erfolglosen Anfragen und weigert sich, diese neu anzufragen, obwohl die Verbindung in das Internet wieder steht. Für diesen Fall sollte man die *minutes* in *seconds* ändern, dann führt auch ein *Reload* im Browser, wenige Sekunden nach der Einwahl, wieder zum Erfolg.

never_direct allow <acl_name> Will man verhindern, dass Squid Anfragen direkt aus dem Internet fordert, kann man hiermit die Verwendung eines anderen Proxies erzwingen. Diesen muss man zuvor unter *cache_peer* eingetragen haben. Gibt man als <*acl_name*> *all* an, erzwingt man, dass sämtliche Anfragen direkt an den *parent* weitergegeben werden. Das kann zum Beispiel nötig sein, wenn man einen Provider verwendet, der die Verwendung seines Proxies zwingend vorschreibt oder die Firewall keinen direkten Zugriff auf das Internet durchlässt.

Optionen zur Zugriffskontrolle

Squid bietet ein detailliertes System, um den Zugriff auf den Proxy zu steuern. Durch die Verwendung von ACLs ist es einfach und vielseitig konfigurierbar. Dabei handelt es sich um Listen mit Regeln, die der Reihe nach abgearbeitet werden. ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs wie *all* und *localhost* sind bereits vorhanden. Das Festlegen einer ACL an sich bewirkt aber noch gar nichts. Erst wenn sie tatsächlich eingesetzt wird, zum Beispiel in Verbindung mit *http_access*, werden die definierten Regeln abgearbeitet.

acl <acl_name> <type> <data> Eine ACL benötigt zur Definition mindestens drei Angaben. Der Name <*acl_name*> kann frei gewählt werden. Für <*type*> kann man aus einer Vielzahl unterschiedlicher Möglichkeiten auswählen, die man im Abschnitt *ACCESS CONTROLS* in der `/etc/squid/squid.conf` nachlesen kann. Was für <*data*> anzugeben ist, hängt vom jeweiligen Typ der ACL ab und kann auch aus einer Datei, zum Beispiel mit Rechnernamen, IP-Adressen oder URLs eingelesen werden. Im folgenden einige einfache Beispiele:

```
acl meinesurfer srcdomain .meine-domain.com
acl lehrer src 192.168.1.0/255.255.255.0
acl studenten src 192.168.7.0-192.168.9.0/255.255.255.0
acl mittags time MTWHF 12:00-15:00
```

http_access allow <acl_name> Mit *http_access* wird festgelegt, wer den Proxy verwenden darf und auf was er im Internet zugreifen darf. Dabei sind ACLs anzugeben, *localhost* und *all* sind weiter oben bereits definiert, die mit *deny* oder *allow* den Zugriff sperren oder freigeben. Man kann hier eine Liste mit vielen *http_access*-Einträgen erstellen, die von oben nach unten abgearbeitet werden; je nachdem, was zuerst zutrifft, wird der Zugriff auf die angeforderte URL freigegeben

oder gesperrt. Als letzter Eintrag sollte immer *http_access deny all* stehen. Im folgenden Beispiel hat *localhost*, also der lokale Rechner, freien Zugriff auf alles, während er für alle anderen komplett gesperrt ist:

```
http_access allow localhost
http_access deny all
```

Noch ein Beispiel, in dem die zuvor definierten ACLs verwendet werden: Die Gruppe `lehrer` hat jederzeit Zugriff auf das Internet, während die Gruppe `studenten` nur Montags bis Freitags, und da nur mittags, surfen darf:

```
http_access deny localhost
http_access allow lehrer
http_access allow studenten mittags
http_access deny all
```

Die Liste mit den eigenen *http_access*-Einträgen sollte man der Übersichtlichkeit halber nur an der dafür vorgesehenen Stelle in der `/etc/squid/squid.conf` eintragen. Das bedeutet zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

und dem abschließenden

```
http_access deny all
```

redirect_program /usr/bin/squidGuard
Mit dieser Option kann man einen „Redirector“ wie squidGuard angeben, der in der Lage ist, unerwünschte URLs zu sperren. In Verbindung mit Proxy-Authentifizierung und den passenden ACLs kann man so den Zugriff auf das Internet für verschiedene Benutzergruppen sehr differenziert steuern. squidGuard ist ein eigenes Paket, das separat zu installieren und konfigurieren ist.

auth_param basic program /usr/sbin/pam_auth
Sollen sich die Benutzer am Proxy authentifizieren müssen, kann man hier ein entsprechendes Programm wie beispielsweise pam_auth angeben. Bei der Verwendung von pam_auth öffnet sich für den Anwender beim ersten Zugriff ein Loginfenster, in dem er Benutzername und Passwort eingeben muss. Zusätzlich ist noch eine ACL erforderlich, damit nur Clients mit gültigem Login surfen können:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Das *REQUIRED* nach *proxy_auth* kann man auch durch eine Liste von erlaubten Benutzernamen oder einen Pfad zu solch einer Liste ersetzen.

ident_lookup_access allow <acl_name>
Hiermit erreicht man, dass auf alle durch die ACL definierten Clients eine Ident-Anfrage ausgeführt wird, um die Identität des jeweiligen Benutzers zu ermitteln. Setzt man für *<acl_name> all* ein, erfolgt dies generell für alle Clients. Auf den Clients muss dazu ein Ident-Daemon laufen, bei Linux kann man dafür das Paket pidentd installieren, für Windows gibt es freie Software, die man sich aus dem Internet besorgen kann. Damit nur Clients mit erfolgreichem Ident-Lookup zugelassen werden, ist auch hier wieder eine entsprechende ACL zu definieren:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Auch hier kann man das *REQUIRED* wieder durch eine Liste erlaubter Benutzernamen ersetzen. Die Verwendung von *Ident* kann den Zugriff merklich verlangsamen, da die Ident-Lookups durchaus für jede Anfrage wiederholt werden.

25.3.6 Konfiguration eines Transparenten Proxy

Normalerweise schickt der Web-Browser an einen bestimmten Port des Proxy-Servers Anfragen und der Proxy stellt die angeforderten Objekte zur Verfügung, ob sie nun im Cache sind oder nicht. Innerhalb eines Netzwerks können verschiedene Situationen auftreten:

- Aus Sicherheitsgründen ist es besser, wenn alle Clients zum Surfen im Internet einen Proxy verwenden.
- Es ist notwendig, dass alle Clients einen Proxy verwenden; dabei ist es gleichgültig, ob sie sich dessen bewusst sind oder nicht.

- In einem Netzwerk wird der Proxy umgezogen, die bestehenden Clients sollen jedoch ihre alte Konfiguration behalten.

In jedem dieser Fälle kann ein transparenter Proxy eingesetzt werden. Das Prinzip ist denkbar einfach: Der Proxy nimmt die Anfragen des Web-Browsers entgegen und bearbeitet sie, sodass der Web-Browser die angeforderten Seiten erhält ohne zu wissen, woher sie kommen. Der gesamte Prozess wird transparent ausgeführt, daher der Name für den Vorgang.

Kernel-Konfiguration

Zuerst sollte sicherstellt sein, dass der Kernel des Proxy-Servers einen Transparenten Proxy unterstützt. Der mit SUSE LINUX Enterprise Server ausgelieferte Kernel ist entsprechend konfiguriert. Andernfalls muss man dem Kernel diese Optionen hinzufügen und ihn neu kompilieren. Genauere Informationen dazu entnehmen Sie bitte dem Kapitel 9 auf Seite 255.

Konfigurationsoptionen in /etc/squid/squid.conf

Folgende Optionen in der Datei `/etc/squid/squid.conf` müssen aktiviert werden, um einen Transparenten Proxy aufzusetzen:

- `httpd_accel_host` virtual
- `httpd_accel_port` 80 # Port, auf dem sich der tatsächliche HTTP-Server befindet.
- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

Firewall-Konfiguration mit SuSEfirewall2

Alle durch die Firewall eingehenden Anfragen müssen mithilfe einer Port-Weiterleitungsregel an den Squid-Port weitergeleitet werden. Dafür eignet sich das mitgelieferte Tool SuSEfirewall2. Dessen Konfigurationsdatei findet man in der Datei `/etc/sysconfig/SuSEfirewall2`. Die Konfigurationsdatei wiederum setzt sich aus gut dokumentierten Einträgen zusammen. Auch wenn wir nur einen Transparenten Proxy einrichten wollen, müssen wir einige Firewall-Optionen konfigurieren:

- Gerät zeigt auf Internet: `FW_DEV_EXT`="eth1"
- Gerät zeigt auf Netzwerk: `FW_DEV_INT`="eth0"

Auf Ports und Dienste (siehe `/etc/services`) in der Firewall wird von nicht vertrauenswürdigen Netzwerken also dem Internet zugegriffen. In diesem Beispiel bieten wir lediglich Web-Dienste nach außen hin an:

`FW_SERVICES_EXT_TCP`="www"

Auf Ports/Dienste (siehe `/etc/services`) in der Firewall wird vom sicheren Netzwerk sowohl TCP als auch mit UDP zugegriffen:

`FW_SERVICES_INT_TCP`="domain www 3128"

`FW_SERVICES_INT_UDP`="domain"

Wir greifen auf Web-Dienste und Squid (dessen Standardport ist `3128`) zu. Der oben beschriebene Dienst „Domain“ steht für DNS oder Domain Name Service. Es ist üblich, diesen Dienst zu nutzen. Andernfalls entfernen wir ihn einfach aus obigem Eintrag und setzen folgende Option auf `no`:

`FW_SERVICE_DNS`="yes"

Die wichtigste Option ist die Ziffer `15`:

Beispiel 25.1: *Option 15 der Firewallkonfiguration*

```
#
# 15.)
# Welcher Zugriff auf die einzelnen Dienste soll an einen lokalen
# Port auf dem Firewall-Rechner umgeleitet werden?
#
# Damit können alle internen Benutzer gezwungen werden, über den
# Squid-Proxy zu surfen oder es kann eingehender Webverkehr
# transparent an einen sicheren Web-Server umgeleitet werden.
#
# Wahl: keinen Eintrag vornehmen oder folgend erklärte Syntax von
# Umleitungsregeln, getrennt durch Leerzeichen, verwenden.
# Eine Umleitungsregel besteht aus 1) Quelle IP/Netz, 2) Ziel
# IP/Netz, 3) ursprünglicher Zielport und 4) lokaler Port, an den
# der Verkehr umgeleitet werden soll, getrennt durch Kommata, z.B.:
# "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

Im obigen Kommentar wird die einzuhaltende Syntax gezeigt. Zuerst greifen die IP-Adresse und die Netzwerkmaske der „internen Netzwerke“ auf die Proxy-Firewall zu. Dann die IP-Adresse und die Netzwerkmaske, an die Anfragen von den Clients „gesendet“ werden. Im Fall von Web-Browsern wählt man die Netzwerke `0/0`. Dies ist eine Wildcard und bedeutet „überallhin“. Danach kommt der „ursprüngliche“ Port, an den diese Anfragen geschickt wurden, und schließlich folgt der Port, an den die Anfragen „umgeleitet“ wurden.

Da Squid mehr Protokolle unterstützt als nur HTTP, können auch Anfragen von anderen Ports an den Proxy umgeleitet werden, so zum Beispiel FTP (Port 21), HTTPS oder SSL (Port 443).

Im konkreten Fall werden Web-Dienste (Port `80`) auf den Proxy-Port (hier `3128` umgeleitet. Falls mehrere Netzwerke oder Dienste hinzugefügt werden sollen, müssen diese durch ein Leerzeichen im entsprechenden Eintrag getrennt werden.

```
FW_REDIRECT_TCP="192.168.0.0/16,0/0,80,3128
192.168.0.0/16,0/0,21,3128"
```

```
FW_REDIRECT_UDP="192.168.0.0/16,0/0,80,3128
192.168.0.0/16,0/0,21,3128"
```

Zum Starten der Firewall und der neuen Konfiguration muss man einen Eintrag in der Datei `/etc/sysconfig/SuSEfirewall2` editieren. Der Eintrag `START_FW` muss auf "yes" gesetzt werden:

Starten Sie Squid wie in Abschnitt 25.3.4 auf Seite 664 beschrieben. Anhand der Protokoll-Dateien in `/var/log/squid/access.log` kann überprüft werden, ob alles richtig funktioniert. Um zu überprüfen, ob alle Ports korrekt konfiguriert wurden, kann von jedem beliebigen Rechner außerhalb unserer Netzwerke auf dem Rechner ein Portscan ausgeführt werden. Nur der Web-Dienst-Port (80) sollte offen sein. Der Portscan führt über `nmap -O` ⟨*IP-Adresse*⟩.

25.3.7 cachemgr.cgi

Der Cache-Manager (cachemgr.cgi) ist ein CGI-Hilfsprogramm zur Ausgabe von Statistiken über den benötigten Speicher des laufenden Squid-Prozesses. Im Gegensatz zum Protokollieren erleichtert dies die Cache-Verwaltung und die Anzeige von Statistiken.

Einrichten

Zuerst wird ein lauffähiger Web-Server auf dem System benötigt. Als Benutzer `root` gibt man Folgendes ein, um herauszufinden, ob Apache bereits läuft: `rcapache status`.

Erscheint eine Nachricht wie die folgende, läuft Apache auf dem Rechner:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Andernfalls müssen Sie folgenden Befehl eingeben: `rcapache start`. So wird Apache mit den Standardeinstellungen von SUSE LINUX gestartet.

Als letzten Schritt muss man die Datei `cachemgr.cgi` aus dem Verzeichnis `/usr/share/doc/packages/squid/scripts/` in das Verzeichnis `/srv/www/cgi-bin` von Apache kopieren.

Cache-Manager ACLs in /etc/squid/squid.conf

Folgende Standardeinstellungen sind für den Cache-Manager erforderlich:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Folgende Regeln sollten enthalten sein:

```
http_access allow manager localhost
http_access deny manager
```

Die erste ACL ist am wichtigsten, da der Cache-Manager versucht, mit dem Squid über das cache_object-Protokoll zu kommunizieren. Die folgenden Regeln setzen voraus, dass der Web-Server und Squid auf demselben Rechner laufen. Die Kommunikation zwischen dem Cache-Manager und Squid entsteht beim Web-Server, nicht beim Browser. Befindet sich der Web-Server also auf einem anderen Rechner, müssen Sie extra eine ACL wie in der Beispieldatei 25.2 hinzufügen.

Beispiel 25.2: *Zugriffsregeln*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP Webserver
```

Dann werden noch folgende Regeln aus Datei 25.3 benötigt.

Beispiel 25.3: *Zugriffsregeln*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Es ist auch möglich, ein Passwort für den Manager zu konfigurieren, wenn auf mehrere Optionen zugegriffen werden soll, wie z. B. Schließen des Cache von Remote oder Anzeigen weiterer Informationen über den Cache. Dann müssen Sie den Eintrag `cachemgr_passwd` und die Optionenliste, die angezeigt werden soll, mit einem Passwort für den Manager konfigurieren. Diese Liste erscheint als Teil der Eintragkommentare in `/etc/squid/squid.conf`.

Immer wenn sich die Konfigurationsdatei geändert hat, muss Squid neu gestartet werden. Dies geschieht am einfachsten mit dem Befehl:
`rcsquid reload`

Statistiken anzeigen

Gehen Sie zur entsprechenden Web-Seite, beispielsweise `http://webserver.example.org/cgi-bin/cachemgr.cgi` Drücken Sie auf 'continue' und lassen Sie sich die verschiedenen Statistiken anzeigen. Weitere Informationen über die einzelnen Einträge, die vom Cache-Manager ausgegeben werden, finden sich in den FAQs zu Squid: `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`

25.3.8 squidGuard

Dieses Kapitel soll lediglich eine Einführung zur Konfiguration von squidGuard sowie ein paar Ratschläge zu dessen Einsatz geben. Auf eine umfangreiche Erklärung wird an dieser Stelle verzichtet. Tiefer gehende Informationen finden sich auf den Webseiten zu squidGuard: `http://www.squidguard.org`

squidGuard ist ein freier (GPL), flexibler und ultraschneller Filter, ein Umleiter und „PlugIn“ zur Zugriffskontrolle für Squid. Er ermöglicht das Festlegen einer Vielzahl von Zugriffsregeln mit unterschiedlichen Beschränkungen für verschiedene Benutzergruppen für einen Squid-Cache. squidGuard verwendet die Standardschnittstelle von Squid zum Umleiten. squidGuard kann u. a. für Folgendes verwendet werden:

- Beschränkung des Internetzugriffs für einige Benutzer auf bestimmte akzeptierte/bekannte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf bestimmte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf URLs, die bestimmte reguläre Ausdrücke oder Wörter enthalten.

- Umleiten gesperrter URLs an eine „intelligente“ CGI-basierte Infoseite.
- Umleiten nicht registrierter Benutzer an ein Registrationsformular.
- Umleiten von Bannern an ein leeres GIF.
- Unterschiedliche Zugriffsregeln abhängig von der Uhrzeit, dem Wochentag, dem Datum etc.
- Unterschiedliche Regeln für die einzelnen Benutzergruppen.

Weder mit squidGuard noch mit Squid ist Folgendes möglich:

- Text innerhalb von Dokumenten filtern, zensieren oder editieren.
- In HTML eingebettete Skriptsprachen wie JavaScript oder VBscript filtern, zensieren oder editieren.

Installieren Sie das `squidGuard`. Editieren Sie die Konfigurationsdatei `/etc/squidguard.conf`. Es gibt zahlreiche andere Konfigurationsbeispiele unter `http://www.squidguard.org/config/`. Sie können später mit komplizierteren Konfigurationseinstellungen experimentieren.

Der nächste Schritt besteht darin, eine Dummy-Seite „Zugriff verweigert“ oder eine mehr oder weniger aufwendige CGI-Seite zu erzeugen, um Squid umzuleiten, falls der Client eine verbotene Webseite anfordert. Der Einsatz von Apache wird auch hier wieder empfohlen.

Nun müssen wir Squid so einstellen, dass er squidGuard benutzt. Dafür verwenden wir folgende Einträge in der Datei `/etc/squid/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Eine andere Option namens `redirect_children` konfiguriert die Anzahl der verschiedenen auf dem Rechner laufenden „Redirects“, also Umleitungsprozesse (in diesem Fall squidGuard). squidGuard ist schnell genug, um eine Vielzahl von Anfragen zu bearbeiten; squidGuard ist wirklich schnell: 100.000 Anfragen innerhalb von 10 Sekunden sind auf einem 500 MHz Pentium mit 5900 Domains, 7880 URLs, gesamt 13780, sidn möglich. Es wird daher empfohlen, nicht mehr als 4 Prozesse festzusetzen, da die Zuweisung dieser Prozesse unnötig viel Speicher braucht.

```
redirect_children 4
```

Als Letztes lassen Sie den Squid die neue Konfiguration einlesen: `rcsquid reload`. Nun können Sie Ihre Einstellungen in einem Browser testen.

25.3.9 Erzeugen von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, das zur Erzeugung von Aktivitätsberichten des Cache im ASCII- oder HTML-Format verwendet wird. Es arbeitet mit Squid-eigenen Zugriffsprotokolldateien. Die Homepage zu Calamaris befindet sich unter: `http://Calamaris.Cord.de/`. Das Programm ist einfach zu verwenden. Melden Sie sich als `root` an und geben Sie folgenden Befehl ein: `cat access.log.files | calamaris` ⟨*options*⟩ `> reportfile`.

Beim Verketten mehrerer Protokoll-Dateien ist die Beachtung der chronologischen Reihenfolge wichtig, das heisst ältere Dateien kommen zuerst. Die verschiedenen Optionen:

-a Ausgabe aller verfügbaren Berichte.

-w Ausgabe als HTML-Bericht.

-l Nachricht oder Logo im Header des Berichts.

Weitere Informationen über die verschiedenen Optionen finden Sie in der Manual-Page zu calamaris: `man calamaris`.

Ein weiteres, leistungsstarkes Tool zum Erzeugen von Cache-Berichten ist SARG (Squid Analysis Report Generator). . Weitere Informationen dazu gibt es unter: `http://web.onda.com.br/orso/`

25.3.10 Weitere Informationen zu Squid

Besuchen Sie die Homepage von Squid: `http://www.squid-cache.org/`. Hier finden Sie den „Squid User Guide“ und eine sehr umfangreiche Sammlung von FAQs zu Squid. Das Mini-Howto zum Transparenten Proxy in dem Paket `howtoen` finden Sie nach der Installation unter: `/usr/share/doc/howto/en/mini/TransparentProxy.gz`

Des Weiteren gibt es Mailinglisten für Squid unter: `squid-users@squid-cache.org`. Das Archiv dazu befindet sich unter: `http://www.squid-cache.org/mail-archive/squid-users/`.

Sicherheit im Netzwerk

Sicherheit von Daten, Diensten und Transfers in Netzwerken ist und bleibt ein brisantes Thema. Wie Sie sich gegen unauthorisierte Zugriffe und Attacken von außen schützen, erfahren Sie in diesem Kapitel.

Das Einrichten einer CA (engl. *Certification Authority*) ermöglicht den Einsatz verschlüsselter Kommunikation im Netz, z.B. via VPN (engl. *Virtual Private Network*). Masquerading, Firewalling und Kerberos sorgen für einen kontrollierten Datenfluss und -austausch. Die Secure Shell (SSH) gibt dem Benutzer die Möglichkeit, sich über eine verschlüsselte Verbindung auf entfernten Rechnern anzumelden. Neben diesen rein technischen Instruktionen finden Sie zum Abschluss auch einen allgemeinen Abschnitt über Sicherheitsaspekte im Linux-Netzwerk.

26.1 X.509-Zertifizierung mit YaST 680
26.2 VPN mit SUSE LINUX 694
26.3 Masquerading und Firewall 705
26.4 SSH – secure shell, die sichere Alternative 715
26.5 Netzwerkauthentifizierung — Kerberos 721
26.6 Installation und Administration von Kerberos . . . 729
26.7 Sicherheit ist Vertrauenssache 748

26.1 X.509-Zertifizierung mit YaST

Immer mehr Authentifizierungsmechanismen stützen sich auf kryptographische Verfahren. Eine wichtige Rolle spielen dabei digitale Zertifikate, die kryptographische Schlüssel ihren Besitzern zuordnen. Diese Zertifikate werden dabei nicht nur für die Kommunikation verwendet, sondern finden sich z.B. auch auf Firmenausweisen. Die Erzeugung und Verwaltung von Zertifikaten wird meist von „offiziellen“ Stellen übernommen, die dies als käufliche Dienstleistung anbieten. In verschiedenen Fällen kann es aber auch sinnvoll sein, diese Aufgaben selbst zu übernehmen, z.B. wenn eine Firma keine personenbezogenen Daten an Dritte weitergeben möchte. SUSE LINUX bietet für diesen Zweck zwei YaST-Module, die elementare Management-Funktionen für digitale X.509-Zertifikate bereitstellen. In den folgenden Abschnitten erhalten Sie zunächst einen Einblick in die Grundlagen der digitalen Zertifizierung und erfahren dann, wie Sie mit YaST solche Zertifikate erstellen und verwalten können. Der ganze Themenkreis „Digitale Zertifizierung“ an sich ist jedoch recht komplex, so dass bei erschöpfender Behandlung leicht Bücher gefüllt werden könnten. Die nachfolgenden Ausführungen können daher nur einen Einblick gewähren. Für detailliertere Informationen lesen Sie bitte die weiterführende Literatur in den Print-Medien und im Internet, z.B. unter:

- `http://www.ietf.org/html.charters/pkix-charter.html` (englisch)
- `http://www.pca.dfn.de/certify/` (deutsch)

26.1.1 Grundlagen der digitalen Zertifizierung

Die digitale Zertifizierung verwendet kryptographische Verfahren zur Verschlüsselung von Daten, um sie vor dem Zugriff durch unberechtigte Personen zu schützen. Dabei werden die Nutzdaten unter Verwendung eines zweiten Datensatzes, einem sog. „Schlüssel“ (engl. *engl. key*) verschlüsselt. Der Schlüssel wird in einem mathematischen Verfahren auf die Nutzdaten angewendet und ergibt dadurch einen veränderten Datensatz, der den ursprünglichen Inhalt nicht mehr erkennen lässt. Heute wird allgemein die asymmetrische Verschlüsselung eingesetzt (*Public-Key-Verfahren*). Dabei treten Schlüssel immer paarweise auf:

Privater Schlüssel (Private Key) Der private Schlüssel muss beim Schlüsseleigner verbleiben und gut verwahrt werden. Die ungewollte Veröf-

fentlichung des privaten Schlüssels kompromittiert das Schlüsselpaar und macht es unbrauchbar.

Öffentlicher Schlüssel (Public Key)
Der öffentliche Schlüssel wird vom Schlüsseleigner in Umlauf gebracht, damit er von Dritten verwendet werden kann.

Schlüsselauthentizität

Aufgrund der weiten Verbreitung der Public-Key-Verfahren sind viele öffentliche Schlüssel im Umlauf. Für den erfolgreichen Einsatz ist es notwendig, dass jeder Teilnehmer verlässlich weiss, dass ein öffentlicher Schlüssel tatsächlich dem unterstellten Besitzer gehört. Die Zuordnung von Besitzer und öffentlichem Schlüssel wird von vertrauenswürdigen Instanzen mittels Public-Key-Zertifikaten bestätigt. Solche Zertifikate enthalten den Namen des Schlüsseleigners, den zugehörigen öffentlichen Schlüssel und die Signatur (elektronische Unterschrift) des Zertifikat-Ausstellers. Vertrauenswürdige Instanzen sind üblicherweise Teil einer Zertifikatsinfrastruktur, die neben dem Ausstellen und Signieren der Zertifikate auch für das übrige Zertifikatsmanagement zuständig ist. Dazu gehören auch Veröffentlichung, Rückruf und Erneuerung von Zertifikaten. Eine solche Infrastruktur wird allgemein als *Public-Key-Infrastruktur* oder kurz *PKI* bezeichnet. Eine bekannte PKI ist der *OpenPGP*-Standard, bei dem die Anwender ohne zentrale Autorisierungsstellen ihre Zertifikate selbst veröffentlichen. Vertrauenswürdig werden diese Zertifikate durch „gegenseitige“ Signierung im „Netz des Vertrauens“ (engl. *Web of Trust*).

Ein alternatives Modell ist die hierarchisch strukturierte *X.509 Public Key Infrastructure* (PKIX), die von der *IETF* (engl. *Internet Engineering Task Force*) definiert wurde und heute als Vorbild für fast alle öffentlich genutzten PKIs dient. Die Authentifizierung erfolgt in diesem Modell in einer hierarchisch-baumartigen Struktur durch sog. *Certification Authorities* (CA). Die Wurzel des Baumes ist die Root-CA, die alle Sub-CAs der nächsten Ebene zertifiziert. Diese Sub-CAs zertifizieren ihrerseits die Sub-CAs der nächsten Ebene, bis schließlich die Sub-CAs der untersten Ebene die Anwender-Zertifakte ausstellen. Die Anwender-Zertifikate erhalten ihre Vertrauenswürdigkeit also durch die Zertifizierung durch die nächsthöheren Sub-CAs, die ihrerseits von den höheren Ebenen der Hierarchie beglaubigt wurden. Auf diese Weise entsteht ein „Zertifizierungspfad“, der bei der Root-CA endet. Die Sicherheit einer solchen PKI steht und fällt daher mit der Vertrauenswürdigkeit der CA-Zertifikate. Um die Zertifizierungsgepflogenheiten für den PKI-Kunden transparent zu machen, definiert der

PKI-Betreiber ein *Certification Practice Statement* (CPS), in dem die Verfahrensweisen beim Zertifikatsmanagement festgelegt sind. Damit soll sichergestellt werden, dass die PKI nur wirklich vertrauenswürdige Zertifikate ausstellt.

X.509-Zertifikate

Ein X.509-Zertifikat ist eine Datenstruktur mit mehreren festen Feldern und (optional) zusätzlichen Ertweiterungsfeldern (Extensions). Die festen Felder enthalten hauptsächlich den Namen des Schlüsselbesitzers, dessen öffentlichen Schlüssel und die Daten der ausstellenden CA (Name und Signatur). Aus Sicherheitsgründen sollte ein Zertifikat nur eine begrenzte Gültigkeitsdauer haben. Auch für dieses Datum ist daher ein Feld vorgesehen. Die CA garantiert die Gültigkeit des Zertifikats im dort angegebenen Zeitraum. Das CPS legt üblicherweise fest, dass die PKI (also letztendlich die CA) noch vor Ablauf der Gültigkeit ein neues Zertifikat erzeugt und verteilt.

Die Erweiterungsfelder können beliebige Zusatzinformationen enthalten. Eine Anwendung muss eine Erweiterung normalerweise nicht auswerten können, es sei denn, sie ist als *kritisch* gekennzeichnet. Kennt eine Anwendung eine kritische Erweiterung nicht, muss sie das Zertifikat zurückweisen. Einige Extensions reduzieren die Verwendung des Zertifikats auf eine bestimmte Anwendung, z.B. Signatur oder Verschlüsselung.

Die Tabelle 26.1 zeigt den prinzipiellen Aufbau eines X.509-Zertifikats in der Version 3.

Tabelle 26.1: *X.509v3-Zertifikat*

Feld	Inhalt
Version	Die Version des Zertifikats, z.B. v3.
Serial Number	Eindeutige ID des Zertifikats (Integer).
Signature	Die ID des Algorithmus, mit dem das Zertifikat signiert wurde.
Issuer	Eindeutiger Name (DN) des Herausgebers (CA)
Validity	Gültigkeitszeitraum (von...bis).
Subject	Eindeutiger Name (DN) des Besitzers.
Subject Public Key Info	Öffentlicher Schlüssel des Besitzers und die ID des Algorithmus.

Issuer Unique ID	Eindeutige ID der ausstellenden CA (optional).
Subject Unique ID	Eindeutige ID des Besitzers (optional)
Extensions	Optionale Zusatzinformationen, z.B. „KeyUsage“, „BasicConstraints“ usw.

X.509-Zertifikate sperren

Wenn ein Zertifikat noch vor Ablauf der Gültigkeitsdauer seine Vertrauenswürdigkeit verliert, muss es umgehend gesperrt werden. Dies ist z.B. dann notwendig, wenn der private Schlüssel öffentlich bekannt wurde. Das gilt in besonderem Maße, wenn der private Schlüssel nicht zu einem Anwenderzertifikat, sondern zu einer CA gehört. In diesem Fall müssen sofort alle Anwenderzertifikate, die von der betroffenen CA ausgestellt wurden, gesperrt werden. Wird ein Zertifikat gesperrt, muss die PKI (genauer die zuständige CA) diese Information allen Beteiligten zur Verfügung stellen. Das gängige Instrument hierfür sind *Certificate Revocation Lists* (CRLs), die von der CA in regelmäßigen Abständen an öffentlichen CRL-Verteilungspunkten (CDP, engl. *CRL Distribution Point*) bereitgestellt werden. Optional kann der CDP auch als Extension im Zertifikat genannt werden, sodass der Prüfer für die Validierung eine aktuelle CRL von dort holen kann. Eine Möglichkeit, dies zu tun, ist das *Online Certificate Status Protocol* (OCSP). Die Authentizität der CRLs wird über die Signatur der ausstellenden CA sichergestellt. Die Tabelle 26.2 zeigt den prinzipellen Aufbau einer X.509-CRL.

Tabelle 26.2: *X.509-Zertifikat-Rückrufliste (CRL)*

Feld	Inhalt
Version	Die Version der CRL, z.B. v2.
Signature	Die ID des Algorithmus, mit dem die CRL signiert wurde.
Issuer	Eindeutiger Name (DN) des CRL-Herausgebers (meist die ausstellende CA).
This Update	Herausgabezeitpunkt (Datum, Uhrzeit) dieser CRL.
Next Update	Herausgabezeitpunkt (Datum, Uhrzeit) der nächsten CRL.

List of revoked Certificates	Liste der zurückgerufenen Zertifikate. Jeder Eintrag enthält die Seriennummer des Zertifikats, den Rückrufzeitpunkt und optionale Erweiterungen (CRL Entry Extensions).
Extensions	Optionale CRL-Erweiterungen.

Repository für Zertifikate und CRLs

Die Zertifikate und CRLs einer CA müssen für ihre Verwendung öffentlich zugänglich gemacht werden. Dies geschieht in einem sog. *Repository*. Weil die Zertifikate und CRLs durch ihre Signatur fälschungssicher sind, muss das Repository selbst nicht in einer speziellen Weise abgesichert werden. Im Gegenteil, ein möglichst einfacher und schneller Zugriff ist anzustreben. Aus diesem Grund werden Zertifikate oft über einen LDAP- oder HTTP-Server bereitgestellt. Erläuterungen zu LDAP finden Sie im Abschnitt 21.8 auf Seite 521. Kapitel 22 auf Seite 581 bietet Informationen zum HTTP-Server.

Die eigene PKI

YaST enthält Module für das elementare Management von X.509-Zertifikaten. Dies beinhaltet vor allem die Erzeugung von CAs, Sub-CAs und deren Zertifikaten. Es sei an dieser Stelle aber erwähnt, dass die Leistungen einer PKI weit über das alleinige Erzeugen und Verteilen der Zertifikate und CRLs hinausgeht. Das Betreiben einer PKI ist eine Dienstleistung, die auch eine durchdachte Verwaltungsinfrastruktur erfordert. Die ständige Pflege der Zertifikate und CRLs erfordert eine recht aufwändige Wartungsarbeit, die von kommerziellen PKI-Produkten erbracht und zum Teil auch automatisiert werden kann. Die YaST-Funktionalität zur Erzeugung und Verteilung von CAs und Zertifikaten kann diese Hintergrund-Organisation aktuell nicht leisten. Ganz allgemein sind die derzeit unter Open-Source verfügbaren PKI-Produkte den kommerziellen Versionen unterlegen. Wenn Sie also eine „kleine“ PKI aufsetzen wollen, können Sie dies mit den nachfolgend beschriebenen YaST-Modulen tun. Für die Einrichtung einer „offiziellen“ — vielleicht auch kommerziellen — PKI sollten Sie aber auf kommerzielle Produkte zurückgreifen.

26.1.2 YaST-Module für CA-Management

YaST stellt zwei Module für elementares CA-Management bereit. Die Funktionalität dieser beiden Module wird nachfolgend an Hand der wichtigsten Tätigkeiten bei der Verwaltung von CAs erläutert.

Root-CA erzeugen

Der erste Schritt für die Einrichtung einer PKI ist die Erzeugung einer Root-CA. Dies geschieht mit dem YaST-Modul 'CA Management' im YaST-Kontrollzentrum unter der Rubrik 'Sicherheit und Benutzer'. Nach dem Start des Moduls sehen Sie zunächst eine Liste aller bereits vorhandenen CAs. Mit dem Button 'Root-CA erzeugen' gelangen Sie in den ersten von drei Dialogen zur Eingabe der CA-relevanten Daten. Im ersten Dialog können Sie die Grunddaten der CA eingeben (Abb. 26.1). Der 'Common Name' ist der „sprechende" Name der CA, also jener, mit dem sie benannt wird. Das Feld 'CA-Name' gibt dagegen den technischen Namen der CA an. Hiervon werden unter anderem Verzeichnisnamen abgeleitet, weshalb hier auch nur die in der Hilfe genannten Zeichen verwendet werden dürfen. Der technische Name wird auch in der Übersichtsliste beim Start des Moduls angezeigt. Es können mehrere E-Mail-Adressen eingegeben werden, die für den CA-Anwender sichtbar sind. Dies kann für Rückfragen hilfreich sein. Als 'Land' sollten Sie jenes auswählen, in dem die CA betrieben wird.

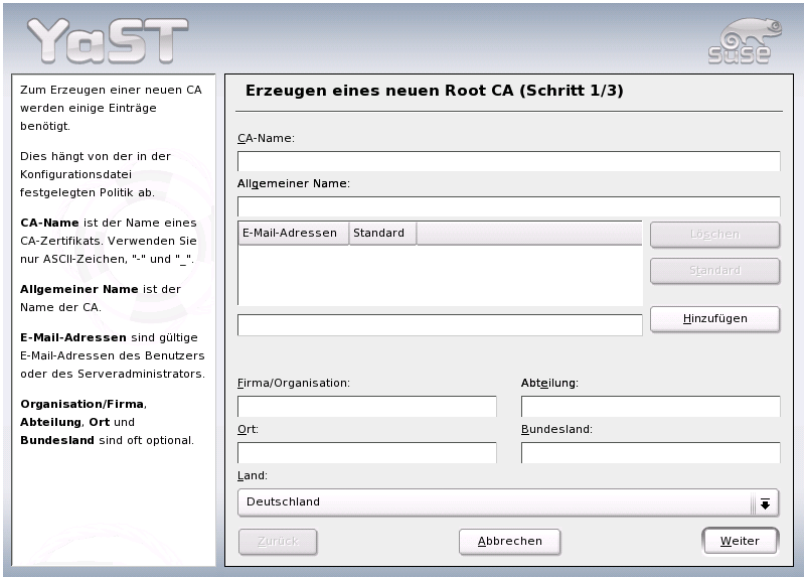

Abbildung 26.1: *YaST CA-Modul - Grunddaten einer Root-CA*

Nach einem Klick auf 'Weiter' müssen Sie im zweiten Dialog ein Passwort eingeben. Dieses Passwort wird immer dann benötigt, wenn Sie die CA

benutzen wollen, d.h. wenn sie z.B. eine Sub-CA anlegen oder Zertifikate erzeugen wollen. Die 'Schlüssellänge' ist bereits sinnvoll vorbelegt und muss im Allgemeinen nicht geändert werden, es sei denn, eine Anwendung kommt mit dieser Schlüssellänge nicht zurecht. Die 'Gültigkeitsdauer' ist bei einer CA mit 3650 Tagen, also ca. 10 Jahren vorgegeben. Diese lange Zeit ist sinnvoll, weil das Ersetzen einer erloschenen CA einen sehr großen administrativen Aufwand nach sich zieht. Mit einem Klick auf den Button 'Erweitert' gelangen Sie in einen Dialog zum Einstellen verschiedener Attribute aus den X.509-Extensions (Abb. 26.4 auf Seite 690). Diese Werte sind sinnvoll voreingestellt und sollten von Ihnen nur verändert werden, wenn Sie genau wissen, was Sie tun.

Im dritten und letzten Schritt zeigt YaST die aktuellen Einstellungen zur Kontrolle noch einmal an. Wenn Sie hier auf 'Erzeugen' klicken, wird die Root-CA angelegt und danach in der Übersichtsliste angezeigt.

Hinweis

Im Allgemeinen ist es sinnvoll, Anwender-Zertifikate nicht von der Root-CA ausstellen zu lassen. Besser ist es, mindestens eine Sub-CA anzulegen, und die Anwender-Zertifikate von dort zu erzeugen. Dies hat den Vorteil, dass die Root-CA isoliert und sicher verwahrt werden kann, z.B. auf einem isolierten Rechner in gut verschlossenen Räumen. Auf diese Weise wird ein Angriff auf die Root-CA sehr erschwert.

Hinweis

Sub-CA erzeugen oder widerrufen

Das Anlegen einer Sub-CA erfolgt genau wie das Anlegen einer Root-CA, mit dem Unterschied, dass vorher jene CA ausgewählt werden muss, in der die Sub-CA erzeugt werden soll. In der Übersichtsliste wählen Sie dazu nach dem Programmstart die gewünschte CA und klicken dann auf 'CA betreten'. Beim erstmaligen Betreten einer CA seit Programmstart müssen Sie das Passwort der CA eingeben und gelangen so in einen Dialog, der die wichtigsten CA-Informationen anzeigt (Abb. 26.2 auf der nächsten Seite). Klicken Sie hier auf den Button 'Erweitert...' und wählen Sie in der Liste 'Sub-CA erzeugen'. Damit kommen Sie dann wieder zum gleichen Dialog, wie beim Anlegen einer Root-CA.

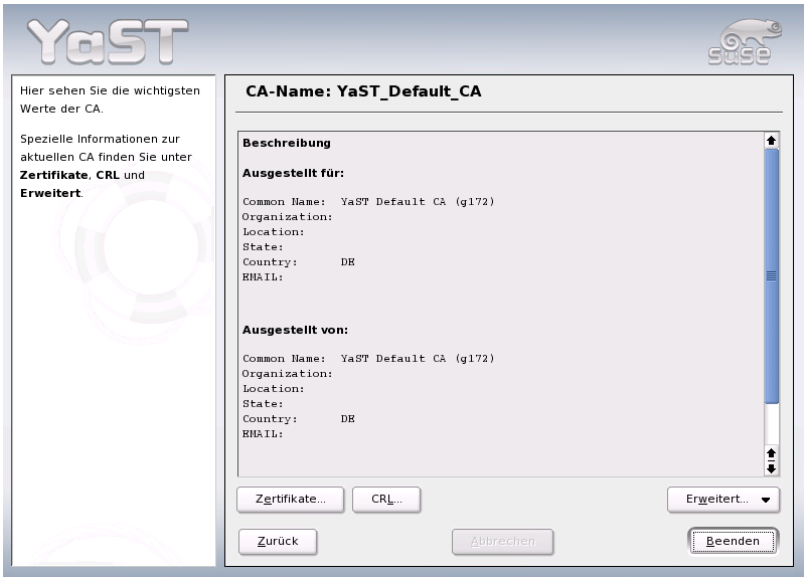

Abbildung 26.2: *YaST CA-Modul - CA verwenden*

Hinweis

Die Gültigkeitsdauer einer Sub-CA muss vollständig innerhalb der Gültigkeitsdauer der „Eltern"-CA liegen. Da eine Sub-CA immer **nach** der „Eltern"-CA erzeugt wird, führt der unkorrigierte Standardwert zu einer Fehlermeldung. Um dies zu vermeiden, geben Sie für die Gültigkeitsdauer einen zulässigen Wert ein.

Hinweis

Nach der Auswahl von 'Zertifikate' sehen Sie den Dialog zur Verwaltung der CA-Zertifikate und Sub-CAs. Dort können Sie mit dem Button 'Widerrufen' kompromittierte oder anderweitig unerwünschte Sub-CAs auch wieder zurückziehen. Der Widerruf alleine ist jedoch noch nicht hinreichend, um eine Sub-CA zu deaktivieren. Sie müssen zurückgezogene Sub-CAs auch in einer CRL veröffentlichen. Die Erzeugung von CRLs wird im Abschnitt 26.1.2 auf Seite 690 beschrieben.

Anwendungszertifikate erzeugen oder widerrufen

Für das Erzeugen von Client- und Server-Zertifikaten muss zunächst eine CA betreten werden, wie es im Abschnitt 26.1.2 auf Seite 686 bereits beschrieben wurde. Anwendungszertifikate sollten dabei nur in Sub-CAs erzeugt werden, weil dann die Root-CA getrennt und sicher verwahrt werden kann. Nach einem Klick auf 'Zertifikate...' sehen Sie den Dialog zur Verwaltung der Zertifikate (Abb. 26.3 auf der nächsten Seite). Der obere Teil enthält eine Liste der bereits vorhandenen Zertifikate, darunter werden die Daten des aktuell selektierten Zertifikats angezeigt. Mit dem Button 'Hinzufügen' können Sie Client- und Server-Zertifikate neu erzeugen und in die Liste der CA aufnehmen. Die Dialoge zur Datenerfassung sind wieder ganz ähnlich jenen zum Anlegen der CAs, und es gilt sinngemäß das dort bereits gesagte. Zusätzliche Anmerkungen betreffen die E-Mail-Adressen in Zertifikaten, die für E-Mail-Signatur und -Verschlüsselung gedacht sind. Für die Signatur sollte die E-Mail-Adresse des Senders (also des Private-Key-Besitzers) im Zertifikat enthalten sein, damit das Mail-Programm das richtige Zertifikat zuordnen kann. Für die Zertifikat-Zuordnung beim Verschlüsseln ist es notwendig, dass die E-Mail-Adresse des Empfängers (also des Public-Key-Besitzers) enthalten ist. Außerdem muss bei Server-Zertifikaten im Feld 'Common Name' unbedingt der Hostname des Servers eingetragen werden. Die Gültigkeitsdauer ist bei Zertifikaten auf 365 Tage voreingestellt.

Hinweis

Wenn Zertifikate für IPsec-Anwendungen mit Windows-XP erstellt werden sollen, müssen dafür **Client**-Zertifikate verwendet werden. Dort hat das Extension-Feld „KeyUsage“ jene Werte, die von Windows erwartet werden.

Hinweis

Mit dem Button 'Widerrufen' können Sie hier auch kompromittierte oder anderweitig unerwünschte Zertifikate zurückziehen. Der Widerruf alleine ist jedoch noch nicht hinreichend, um ein Zertifikat zu deaktivieren. Sie müssen zurückgezogene Zertifikate auch in einer CRL veröffentlichen. Die Erzeugung von CRLs wird im Abschnitt 26.1.2 auf Seite 690 beschrieben. Zurückgezogene Zertifikate können **nach** der Veröffentlichung in einer CRL mit dem Button 'Löschen' auch komplett entfernt werden.

Standardwerte verändern

In den vorigen Abschnitten wurde erläutert, wie Sie Sub-CAs, Client-Zertifikate und Server-Zertifikate erzeugen können. Dabei kommen jeweils

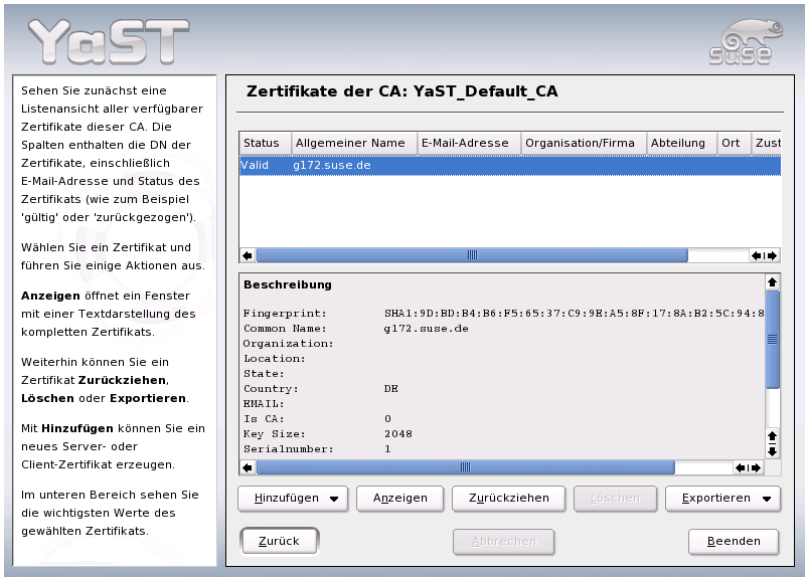

Abbildung 26.3: *Zertifikate einer CA*

spezielle Einstellungen in den Extension-Feldern des X.509-Zertifikats zur Anwendung. Diese Einstellungen wurden für jeden Zertifikat-Typ sinnvoll voreingestellt und müssen normalerweise nicht verändert werden. Es kann jedoch sein, dass eine bestimmte Anwendung spezielle Anforderungen an den Inhalt dieser Extension-Felder stellt. Wenn Sie für eine solche Anwendung wiederholt Zertifikate erzeugen wollen, ist es vielleicht sinnvoll, die Voreinstellungen anzupassen. Andernfalls müssten Sie das bei jeder Zertifikat-Erzeugung von neuem tun.

Das System verwaltet für jede CA einen Satz von Voreinstellungen für die Erzeugung von Sub-CAs, Client-Zertifikaten und Server-Zertifikaten. Um diese Voreinstellungen zu verändern, müssen Sie die gewünschte CA betreten, wie es im Abschnitt 26.1.2 auf Seite 686 bereits beschrieben wurde. Dort finden Sie nach einem Klick auf den Button ‘Erweitert’ die Option ‘Voreinstellungen’ und können dann auswählen, für welchen Typ die Einstellungen geändert werden sollen. Danach gelangen Sie in den Dialog zum Ändern der jeweiligen Vorgaben (Abb. 26.4 auf der nächsten Seite).

Auf der linken Seite sehen Sie die Baumstruktur mit allen systembekannten Extension-Feldern. Wenn Sie hier ein Feld anklicken, können Sie im rech-

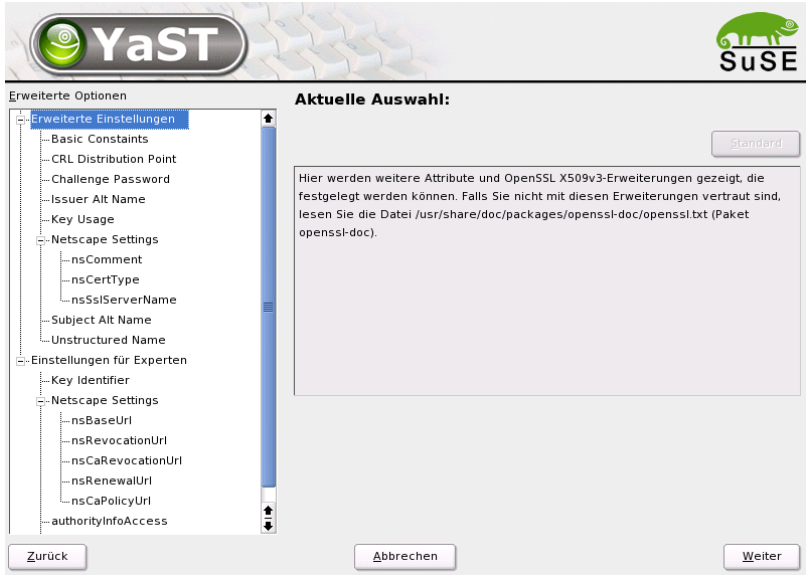

Abbildung 26.4: *YaST CA-Modul - Erweiterte Einstellungen*

ten Teil den zugehörigen Wert ändern und mit der Checkbox ‘kritisch’ die „critical“-Markierung setzen oder löschen. Nach einem Klick auf ‘Weiter’ sehen Sie eine kurze Zusammenfassung und können mit ‘Speichern’ Ihre Änderungen sichern.

Hinweis

Alle Änderungen an den Voreinstellungen wirken sich nur auf zukünftig erzeugte Objekte aus. Bereits existierende CAs und Zertifikate bleiben unverändert.

Hinweis

CRLs erzeugen

Wenn kompromittierte oder anderweitig unerwünschte Zertifikate von der weiteren Verwendung ausgeschlossen werden sollen, müssen sie zunächst zurückgezogen werden. Wie dies zu geschehen hat, wurde bereits in den Abschnitten 26.1.2 auf Seite 686 (für Sub-CAs) und 26.1.2 auf Seite 688 (für

Anwendungszertifikate) erläutert. Danach muss **unbedingt** eine CRL mit diesen Informationen erzeugt und veröffentlicht werden.

Das System verwaltet für jede CA genau eine CRL. Um diese CRL zu erzeugen oder zu aktualisieren, betreten Sie zunächst die gewünschte CA, wie es im Abschnitt 26.1.2 auf Seite 686 bereits beschrieben wurde, und klicken dort den Button 'CRL...'. Der folgende Dialog zeigt dann eine Zusammenfassung der letzten CRL dieser CA. Wenn Sie zwischenzeitlich neue Sub-CAs oder Zertifikate zurückgezogen haben, müssen Sie eine neue CRL erzeugen, damit diese Information in die CRL aufgenommen wird. Um die CRL zu erzeugen oder zu aktualisieren wählen Sie 'CRL erzeugen'. Danach können Sie noch die Gültigkeitsdauer für die neue CRL (Vorgabe: 30 Tage) angeben, und nach einem Klick auf 'OK' wird die CRL erzeugt und angezeigt. Anschließend müssen Sie diese CRL noch veröffentlichen. Wie das geht, erfahren Sie in den nächsten Abschnitten.

Hinweis

Anwendungen, die CRLs auswerten, weisen Zertifikate zurück, deren CRL erloschen ist. Als PKI-Betreiber haben Sie daher die Pflicht, immer eine neue CRL zu erzeugen und zu veröffentlichen, bevor eine aktuelle CRL erlischt (Gültigkeitsdauer). YaST stellt aktuell keine Funktionalität bereit, um diesen Vorgang zu automatisieren. Sie müssen dies also selbst überwachen.

Hinweis

CA-Objekte nach LDAP exportieren

Für den LDAP-Export sollte der ausführende Rechner mit dem YaST-LDAP-Client konfiguriert sein, weil dann zur Laufzeit LDAP-Server-Informationen vorliegen, die beim Ausfüllen der Dialogfelder verwendet werden. Andernfalls ist der Export zwar trotzdem möglich, jedoch müssen dann alle LDAP-Daten von Hand eingetragen werden. In jedem Fall müssen Sie mehrere Passworte eingeben (siehe Tabelle 26.3).

Tabelle 26.3: *Passworte beim LDAP-Export*

Passwort	Bedeutung
LDAP-Passwort	Dieses Passwort berechtigt zur Eintragung im LDAP-Baum.
Zertifikat-Passwort	Dieses Passwort berechtigt zum Export des Zertifikats.

Neues Zertifikat-Passwort	Beim LDAP-Export kommt das PKCS12-Format zur Anwendung. Dieses Format erzwingt die Vergabe eines neuen Passwortes für das exportierte Zertifikat.

Es können sowohl Zertifikate wie auch CAs und CRLs nach LDAP exportiert werden.

- **CA nach LDAP exportieren**

  Für den Export einer CA betreten Sie die CA, wie es im Abschnitt 26.1.2 auf Seite 686 beschrieben wurde. Im dann folgenden Dialog wählen Sie 'Erweitert' -> 'Export nach LDAP' und gelangen so in den Dialog zur Eingabe der LDAP-Daten. Wenn Ihr System mit dem YaST-LDAP-Client konfiguriert wurde, sind die Felder schon teilausgefüllt, andernfalls müssen Sie alle Daten von Hand eingeben. Die Eintragung in LDAP erfolgt in einem separaten Baum mit dem Attribut „caCertificate".

- **Zertifikat nach LDAP exportieren**

  Betreten Sie hierzu jene CA, die Ihr zu exportierendes Zertifikat enthält und wählen Sie dort 'Zertifikate'. In der Zertifikat-Liste im oberen Teil des Dialogs selektieren Sie das gewünschte Zertifikat und wählen 'Export' -> 'Export nach LDAP'. Die Eingabe der LDAP-Daten erfolgt hier genauso wie bei CAs. Im LDAP-Baum wird dann ein passendes User-Objekt gesucht, und das Zertifikat dort mit den Attributen „userCertificate" (PEM-Format) und „userPKCS12" (PKCS12-Format) gespeichert.

- **CRL nach LDAP exportieren**

  Betreten Sie hierzu jene CA, die Ihre zu exportierende CRL enthält und wählen Sie dort 'CRL...'. Im folgenden Dialog können Sie ggf. eine neue CRL erzeugen und diese dann mit 'Export' -> 'nach LDAP' exportieren. Die Eingabe der LDAP-Daten erfolgt auch hier wie bei CAs. Die Eintragung in LDAP geschieht dann an der gleichen Stelle wie die zugehörige CA, jedoch mit dem Attribut „certificateRevocationList".

CA-Objekte als Datei exportieren

Wenn Sie auf dem Rechner zur CA-Verwaltung ein Repository eingerichtet haben, können Sie mit dieser Option die CA-Objekte gleich als Datei am

richtigen Ort erzeugen. Es stehen verschiedene Ausgabeformate wie z.B. PEM, DER und PKCS12 zur Auswahl. Bei PEM kann auch ausgewählt werden, ob ein Zertifikat mit oder ohne Schlüssel exportiert werden soll, und ob der Schlüssel verschlüsselt sein soll. Bei PKCS12 kann zusätzlich der Zertifizierungspfad mit exportiert werden.

Der Export als Datei wird für Zertifikate, CAs und CRLs genauso durchgeführt, wie schon bei LDAP im Abschnitt 26.1.2 auf Seite 691 beschrieben. Sie müssen nur 'Export als Datei' anstatt 'Export nach LDAP' auswählen. Sie gelangen dann in einen Dialog zur Auswahl des gewünschten Ausgabeformats sowie zur Eingabe der Passworte und des Dateinamens. Nach einem Klick auf 'OK' wird das Zertifikat am gewählten Ort gespeichert.

Hinweis

Sie können hier den Speicherort im Dateisystem beliebig wählen. Diese Option kann daher auch dazu verwendet werden, CA-Objekte z.B. auf einem USB-Stick als Transportmedium zu speichern.

Hinweis

Zertifikate auf Floppy exportieren

Für Zertifikate (nicht CAs oder CRLs) bietet YaST noch die Möglichkeit des Exports auf Floppy. Der Sinn dieser Option ist der bequeme Transport von Server-Zertifikaten von einem isoliert gehaltenen CA-Rechner zu einem Server, der diese Zertifikate verwenden soll. Diese YaST-Funktionalität ist das Gegenstück zu einem speziellen YaST-Modul, das nur dazu dient, solchermaßen exportierte Zertifikate auf dem Server wieder zu importieren (siehe nächsten Abschnitt).

Für den Floppy-Export betreten Sie zunächst jene CA, die Ihre zu exportierenden Zertifikate enthält und wählen dort 'Zertifikate'. Selektieren Sie das gewünschte Zertifikat in der Liste und exportieren Sie es mit 'Export' -> 'Export auf Floppy'. Im nachfolgenden Dialog werden Sie aufgefordert, eine Floppy einzulegen, und können das neue PKCS12-Passwort eingeben. Nach einem Klick auf 'Weiter' wird das Zertifikat dann auf die Floppy geschrieben.

Allgemeines Server-Zertifikat importieren

Wenn Sie auf einem isolierten CA-Verwaltungsrechner mit YaST ein Server-Zertifikat auf Floppy exportiert haben, können Sie dieses Zertifikat auf einem Server als „Allgemeines Server-Zertifikat“ wieder importieren. Dies kann entweder schon während der Installation oder später mit

dem YaST-Modul ‘Allgemeines Server-Zertifikat importieren’ im YaST-Kontrollzentrum unter der Rubrik ‘Sicherheit und Benutzer’ geschehen. Das „Allgemeine Server-Zertifikat“ wird in `/etc/ssl/servercerts` gespeichert und kann dort von beliebigen CA-gestützten Diensten verwendet werden. Wenn dieses Zertifikat erlischt, kann es durch Anwendung der gleichen Mechanismen auf einfache Weise ersetzt werden. An weiterem administrativem Aufwand ist dann nur ein Neustart der beteiligten Dienste notwendig.

Nach dem Start des Moduls sehen Sie zunächst im Beschreibungsfeld die Daten des aktuellen Zertifikats. Für den Import wählen Sie ‘Import’ -> ‘von Floppy’ und legen die entsprechende Diskette ein. Nach der Eingabe des Zertifikat-Passwortes und einem Klick auf ‘Weiter’ wird das Zertifikat importiert und anschließend im Beschreibungsfeld angezeigt.

Hinweis

Wenn Sie hier ‘Import’ -> ‘von Festplatte’ wählen, können Sie die Quelle im Dateisystem frei wählen. Diese Option kann daher auch dazu verwendet werden, Zertifikate z.B. von einem USB-Stick als Transportmedium zu importieren.

Hinweis

26.2 VPN mit SUSE LINUX

VPN (engl. *Virtual Private Network*) bezeichnet eine Technologie, mit der „sichere“ Datenverbindungen über das „unsichere“ Medium Internet realisiert werden können. Die Kommunikation findet dabei nicht **mit** dem Internet statt, sondern **über** das Internet. Die Datenpakete werden hier für Authentifizierung und Vertraulichkeit verschlüsselt und in ein neues Paket verpackt (Tunneling). Auf diese Weise ist es kostengünstig möglich, ein „sicheres“ Netzwerk zwischen geographisch weit verstreuten Rechnern herzustellen. Die Norm für diese Art des Datenverkehrs ist IPSEC (*Internet Protocol Security)*, die unter Linux (neben anderen) durch das Programm FreeS/WAN realisiert wird.

Die Einrichtung einer VPN-Verbindung erfordert bei allen beteiligten Parteien die Verfügbarkeit digitaler Zertifikate, die zur Überprüfung der „Rechtmäßigkeit“ der Verbindung verwendet werden. Solche Zertifikate können Sie unter anderem mit YaST erzeugen und dann für VPN verwenden. Der Abschnitt 26.1 auf Seite 680 erklärt kurz den Hintergrund der digitalen Zertifizierung und erläutert, wie Sie Zertifikate selbst erstellen und

verwalten können. Die nachfolgenden Abschnitte beschreiben, wie Sie mit YaST einen VPN-Server und VPN-Clients unter Linux und Windows einrichten können.

26.2.1 Road Warrior Server einrichten

Ein Road Warrior Server ist eine VPN-Server-Konfiguration, die Verbindungen von beliebigen Clients mit gültigem und signiertem CA-Zertifikat akzeptiert. Um einen Road Warrior Server einzurichten, sind im Wesentlichen drei Schritte notwendig, die im Folgenden erläutert werden:

- Server-Zertifikat auf dem CA-Verwaltungsrechner erzeugen
- Zertifikat auf dem Server-Rechner importieren
- Verbindung auf dem Server einrichten.

Server-Zertifikat erzeugen

Das Server-Zertifikat erstellen Sie mit dem YaST-CA-Management Modul (siehe Abschnitt 26.1.2 auf Seite 688). Das Zertifikat speichern Sie dann zusammen mit dem Schlüssel und allen beteiligten CAs in eine PKCS12-Datei (siehe Abschnitt 26.1.2 auf Seite 692).

Hinweis

Wenn Zertifikate für IPsec-Anwendungen mit Windows-XP erstellt werden sollen, müssen dafür **Client**-Zertifikate verwendet werden. Dort hat das Extension-Feld „KeyUsage“ jene Werte, die von Windows erwartet werden.

Hinweis

Server-Zertifikat auf dem Server importieren

Starten Sie auf dem Server-Rechner das YaST-Modul ‘VPN’ im YaST-Kontrollzentrum unter der Rubrik ‘Sicherheit und Benutzer’. In der Übersicht (Abb. 26.5 auf der nächsten Seite) klicken Sie ‘Zertifikate’ -> ‘Importieren’ und wählen dann Ihre gespeicherte PKCS12-Datei aus. Für den Import müssen Sie das PKCS12-Passwort eingeben. Danach wird das Zertifikat in der Zertifikat-Liste angezeigt und nach einem Klick auf ‘Weiter’ kehren Sie zur Übersicht zurück.

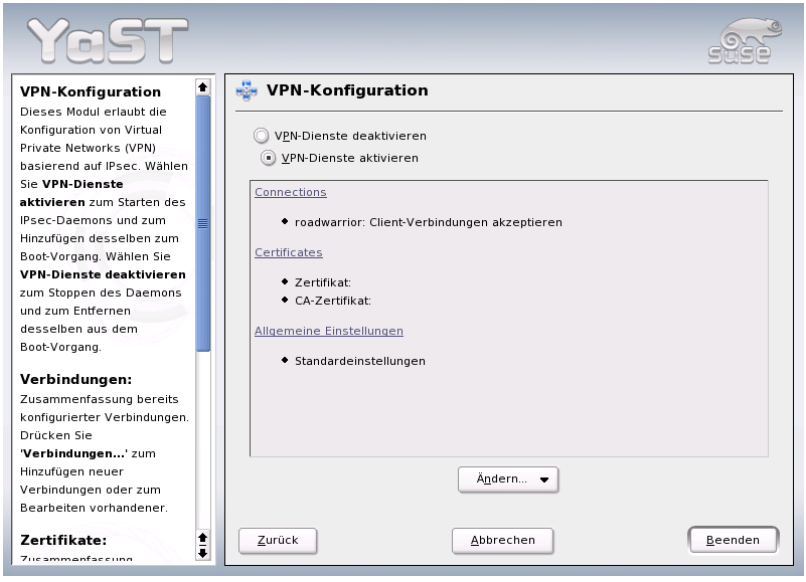

Abbildung 26.5: *YaST VPN-Modul - Übersicht*

Hinweis

Sie sollten hier nicht das „Allgemeine Server-Zertifikat“ des YaST CA-Management-Moduls verwenden, weil IPsec eigene Zertifikate verwaltet.

Hinweis

VPN-Verbindung einrichten

Damit das Zertifikat für IPsec verwendet werden kann, muss noch eine Verbindung dafür eingerichtet werden. Klicken Sie in der Übersicht (Abb. 26.5) auf ‘Verbindungen’ und wählen Sie dann in der Verbindungsübersicht ‘Hinzufügen’. Nach der Auswahl von ‘Road Warrior Server’ wird eine Konfiguration erzeugt, die Verbindungen von beliebigen Clients akzeptiert, wenn sie ein gültiges und von der CA signiertes Zertifikat vorweisen können.

Im nächsten Dialog (Abb. 26.6 auf der nächsten Seite) wählen Sie die Verbindungseinstellungen. Im Feld ‘Lokale IP Adresse’ geben Sie die eigene

IP-Adresse ein. Bei Internet-Einwahlzugängen ist diese jedoch üblicherweise vor der Einwahl nicht bekannt. Allerdings wird bei Internet-Zugängen meist eine Defaultroute gesetzt. Die Einstellung `%defaultroute` weist den Server an, jenes Interface zu benutzen auf das die Defaultroute zeigt. Falls die Verbindung dynamisch auf- und abgebaut werden soll, wenn ein Netzwerk-Interface ohne Defaultroute aktiviert und deaktiviert wird, kann stattdessen `%dynamic` eingetragen werden. Es wird dann die IP Adresses des betreffenden Interfaces verwendet.

Abbildung 26.6: *YaST VPN-Modul - Verbindungseinstellungen*

Soll der Server als Gateway dienen und Clients den Zugriff auf ein Netzwerk ermöglichen, ist das Feld ‘Als Gateway fungieren’ anzukreuzen. Im Eingabefeld müssen Sie dieses Netz dann eintragen, z.B. `10.10.0.0/24`. Sie können hier auch das gewünschte Zertifikat auswählen. Das erste und vielleicht einzige ist bereits vorselektiert.

Hinweis

In diesem vereinfachten Road Warrior Konfigurations-Workflow wird als Identifikation entweder der erste `Subject Alternative Name` (falls vorhanden) oder der `Distinguished Name` aus dem Zertifikat verwendet.

Hinweis

Nach einem Klick auf 'Weiter' können Sie im nächsten Dialog auswählen, wie die Verbindung beim Systemstart behandelt werden soll. Eine Verbindung kann entweder „vorbereitet" oder „ignoriert" werden. Bei einer vorbereiteten Verbindung wartet der Server auf Verbindungsanfragen von Clients. Dies ist nur möglich wenn die lokale IP Adresse schon bekannt ist. Das heißt, im Falle von `%defaultroute` muss die Defaultroute bereits gesetzt sein, und der Rechner muss bereits im Internet eingewählt sein (falls es sich um eine Wählverbindung handelt). Wenn die Verbindung ins Internet nicht schon beim Systemstart hergestellt wird, können Sie auch angeben, dass die Verbindung dynamisch mit einem Netwerkinterface auf- und abgebaut werden soll, z.B. mit einem DSL Interface. Falls es sich bei dem hier gewählten Interface nicht um das Interface der Defaultroute handelt, macht es auch keinen Sinn als lokale IP Adresse `%defaultroute` einzutragen. Nach einem Klick auf 'OK' sehen Sie die neue Verbindung in der Liste der Verbindungsübersicht. Klicken Sie hier noch einmal 'OK' und dann 'Beenden', um die Konfiguration abzuschließen.

26.2.2 VPN-Linux-Client mit FreeS/WAN einrichten

Für die Einrichtung eines VPN-Linux-Clients sind im Wesentlichen drei Schritte notwendig, die im Folgenden erläutert werden:

- Client-Zertifikat auf dem CA-Verwaltungsrechner erzeugen
- FreeS/WAN-Konfigurationsdatei exportieren
- Dateien auf dem Client-Rechner importieren

Client-Zertifikat erzeugen

Das Client-Zertifikat erstellen Sie mit dem YaST CA-Management Modul (siehe Abschnitt 26.1.2 auf Seite 688). Das fertige Zertifikat speichern Sie dann zusammen mit dem Schlüssel und allen beteiligten CAs in eine PKCS12-Datei (siehe Abschnitt 26.1.2 auf Seite 692).

FreeS/WAN-Konfigurationsdatei exportieren

Starten Sie auf dem Server-Rechner das YaST-Modul 'VPN' im YaST-Kontrollzentrum unter der Rubrik 'Sicherheit und Benutzer'. In der Übersicht (Abb. 26.5 auf Seite 696) klicken Sie 'Verbindungen' und selektieren dann in der Verbindungsübersicht die gewünschte Server-Verbindung. Nach der Auswahl von 'Experten...' -> 'Exportieren' -> 'FreeS/WAN' können Sie den Speicherort für die Datei `freeswan_ipsec.conf` bestimmen, die auf den Linux-Client übertragen werden muss. Diese Datei ist ein Vorschlag für einen FreeS/WAN-Client und muss eventuell in Details noch angepasst werden. Die Datei ist auf FreeS/WAN Version 2 zugeschnitten. Ältere Versionen benötigen zusätzliche Parameter.

Dateien auf dem Client importieren

Als nächstes sind die Zertifikate und die Konfigurationsdatei mittels sicherem Medium auf den Client zu übertragen. Die IPsec-Konfigurationsdatei muss auf dem Client-Rechner als `/etc/ipsec.conf` gespeichert werden.

Für den Zertifikat-Import starten Sie auf dem Client-Rechner das YaST-Modul 'VPN' im YaST-Kontrollzentrum unter der Rubrik 'Sicherheit und Benutzer'. In der Übersicht (Abb. 26.5 auf Seite 696) klicken Sie 'Zertifikate' -> 'Importieren' und wählen dann Ihr gespeichertes Client-Zertifikat aus. Für den Import müssen Sie das Passwort des Zertifikats eingeben. Danach wird das Zertifikat in der Zertifikat-Liste angezeigt und nach einem Klick auf 'Weiter' kehren Sie zur Übersicht zurück.

Hinweis

Die Verbindung muss eventuell noch angepasst werden um sie an die lokalen Gegebenheiten anzupassen (z.B. Zertifikat und ID ändern).

Hinweis

Manuelle Client-konfiguration

Wenn der Client-Rechner kein YaST VPN-Modul hat, können die Zertifikate auch von Hand importiert werden:

- Das Client-Zertifikat muss nach `/etc/ipsec.d/certs` kopiert werden.
- Das CA-Zertifikat muss nach `/etc/ipsec.d/cacerts` kopiert werden.

- Der Schlüssel muss nach `/etc/ipsec.d/private` kopiert werden. Nur der Benutzer `root` sollte auf diese Datei zugreifen dürfen, d.h. die Berechtigungen müssen entsprechend angepasst werden.
- Das Passwort für den Schlüssel muss in `/etc/ipsec.secrets` eingetragen sein. Auch diese Datei sollte nur von `root` zugreifbar sein.

Um das Zertifikat aus der PKCS#12-Datei zu extrahieren kann das `openssl` Kommandozeilenprogramm verwendet werden:

```
# openssl pkcs12 -clcerts -nokeys -in DATEI.p12 -out \
          /etc/ipsec.d/certs/cert_01.pem
```

Ebenso das CA-Zertifikat:

```
# openssl pkcs12 -cacerts -nokeys -in DATEI.p12 -out \
          /etc/ipsec.d/cacerts/cacert_01.pem
```

Und auch der Schlüssel:

```
# openssl pkcs12 -nocerts -nodes -in USER.p12 -out \
          /etc/ipsec.d/private/key_01.pem

# chmod 600 /etc/ipsec.d/private/key_01.pem
```

Die option `-nodes` sorgt hier dafür, dass der Schlüssel ohne Passwort abgelegt wird. Dies schadet hier nicht, weil ohnehin nur `root` die Datei lesen kann. In `/etc/ipsec.secrets` ist noch ein Eintrag notwendig, damit FreeS/WAN den Schlüssel kennt:

```
# echo ': RSA /etc/ipsec.d/private/key_01.pem ""' \
         >> /etc/ipsec.secrets

# chmod 600 /etc/ipsec.secrets
```

Nun kann die Konfigurationsdatei nach `/etc/ipsec.conf` kopiert werden. Unter Umständen muss der Dateiname bei `leftcert` angepasst werden. Normalerweise ist jedoch schon `/etc/ipsec.d/certs/cert_01.pem` eingetragen. Der Wert hinter `right` muss mit dem DNS-Hostnamen oder der IP-Adresse des Server Rechners identisch sein.

Mit dem Kommando `rcipsec start` wird IPsec gestartet und die Verbindung aufgebaut (wenn `auto=start` konfiguriert wurde). Mit `ipsec auto --status` oder `setkey -D` sowie durch Inspektion von `/var/log/messages` kann festgestellt werden, ob alles geklappt hat. Mit `rcipsec stop` wird IPsec beendet und alle Verbindungen werden abgebaut.

26.2.3 IPsec-Clients auf Windows XP und Windows 2000

Auch von Windows XP und Windows 2000 Clients aus können Sie IPsec-Verbindungen zu SUSE LINUX einrichten. Die verschiedenen Schritte werden im Folgenden beschrieben.

- Client-Zertifikat auf dem CA-Verwaltungsrechner erzeugen
- Windows-Konfigurationsdatei exportieren
- Windows vorbereiten
- Konfigurieren der Windows Snap-Ins
- Client-Zertifikat importieren
- Wichtige Zertifikat-Daten notieren
- IPsec-Verbindung konfigurieren
- Erzeugen von Desktop-Links

Client-Zertifikat erzeugen

Das Client-Zertifikat erstellen Sie mit dem YaST CA-Management Modul (siehe Abschnitt 26.1.2 auf Seite 688). Das fertige Zertifikat speichern Sie dann zusammen mit dem Schlüssel und allen beteiligten CAs in eine PKCS12-Datei (siehe Abschnitt 26.1.2 auf Seite 692).

Windows-Konfigurationsdatei exportieren

Starten Sie auf dem Server-Rechner das YaST-Modul 'VPN' im YaST-Kontrollzentrum unter der Rubrik 'Sicherheit und Benutzer'. In der Übersicht (Abb. 26.5 auf Seite 696) klicken Sie 'Verbindungen' und selektieren dann in der Verbindungsübersicht die gewünschte Server-Verbindung. Nach der Auswahl von 'Experten...' -> 'Exportieren' -> 'Windows' können Sie den Speicherort für die Datei `windows_ipsec.conf` bestimmen, die auf den Windows-Client übertragen werden muss. Diese Datei ist ein Vorschlag für einen Windows-Client und muss eventuell in Details noch angepasst werden.

Windows vorbereiten

Sie können die IPsec-Verbindung manuell einrichten, hierfür wird das Programm `ipseccmd.exe` (Windows XP) oder `ipsecpol.exe` (Windows 2000) benötigt, das in Ihrer Windows Installation enthalten sein sollte. Bei Windows XP müssen Sie auf der Installations-CD `support\tools\setup.exe` ausführen (Komplett-Installation). Diese Programme sind jedoch kommandozeilenorientiert und somit eher schwierig zu bedienen. Sie können die Verbindung auch über die sog. MMC (engl. *Microsoft Management Console*) konfigurieren, dies ist jedoch nicht besonders intuitiv. Wir empfehlen stattdessen das Tool `ipsec.exe`, das Ihnen die Hauptarbeit bei der Konfiguration der IPsec-Verbindung unter Windows XP oder Windows 2000 abnimmt.

Laden Sie sich dieses Tool unter der URL `http://vpn.ebootis.de/package.zip` auf Ihren Rechner herunter und packen Sie den Inhalt zum Beispiel unter `C:\Programme\IPsec\` aus. Vielen Dank an dieser Stelle an den Autor `marcus@ebootis.de`.

Wenn Sie Windows 2000 verwenden, sollten Sie zuvor mindestens das ServicePack2 einspielen, damit Windows 2000 auch die sog. 3DES-Encryption verarbeiten kann. Ansonsten ist keine Verbindung mit Windows 2000 möglich. Das ServicePack2 erhalten Sie unter der folgenden URL:

```
http://www.microsoft.com/windows2000/downloads/
servicepacks/sp2/sp2lang.asp
```

Weiterhin benötigen Sie bei Windows 2000 das Programm `ipsecpol.exe`, das Sie im sog. Resource Kit oder unter folgender URL finden:

```
http://agent.microsoft.com/windows2000/techinfo/reskit/
tools/existing/ipsecpol-o.asp
```

Hinweis

Dieses Programm installiert sich normalerweise nach `C:/Programme/ResourceKit`. An dieser Stelle nützt es aber wenig, da es ein kommandozeilenorientiertes Programm ist und deshalb in ein Verzeichnis kopiert werden sollte, in dem ausführbare Dateien gespeichert sind. Wir empfehlen das Programm `ipsecpol.exe` nach `C:/WINNT` zu kopieren und die entsprechenden DLLs nach `C:/WINNT/System`. `ipsecpol` muss als Administrator ausgeführt werden.

Hinweis

Konfigurieren der benötigten Windows Snap-Ins

Auf dem Windows-Client öffnen Sie die MMC. Gehen Sie im Start-Menü zu 'Ausführen' -> 'MMC'. Im MMC klicken Sie auf 'Datei' -> 'Snap-In hinzufügen/entfernen'. Ein Dialog öffnet sich, in dem Sie gegebenenfalls aktive Snap-Ins sehen. Klicken Sie auf 'Hinzufügen'. Ein Auswahlfenster wird geöffnet, das alle verfügbaren Snap-Ins anzeigt. Mit 'Zertifikate' -> 'Hinzufügen' gelangen Sie zum Konfigurationsassistent. Hier wählen Sie 'Computerkonto' und klicken auf 'Weiter'. Wählen Sie 'Lokaler Computer' -> 'Fertigstellen' und dann das Snap-In 'IP-Sicherheitsrichtlinienverwaltung' -> 'Hinzufügen'. Es öffnet sich ein Konfigurationsassistent, in dem Sie 'Lokaler Computer' -> 'Fertigstellen' auswählen. Klicken Sie auf 'Schließen' und dann auf 'OK'.

Client-Zertifikat importieren

In der MMC sehen Sie nun die beiden Snap-Ins, die hinzugefügt wurden. Öffnen Sie den Ordner 'Zertifikate'. Klicken Sie mit der rechten Maustaste auf 'Eigene Zertifikate'. Im Dropdown-Menü selektieren Sie 'Alle Tasks' -> 'Importieren'. Der Zertifikat-Assistent wird geöffnet. Wählen Sie hier 'Weiter' -> 'Durchsuchen'. Bei 'Dateityp' geben Sie 'Privater Informationsaustausch' (*.pfx,*.p12) an. Wählen Sie die exportierte PKCS12-Datei aus und klicken Sie auf 'Weiter'. Nun müssen Sie das Passwort eingeben, das Sie im YaST CA-Management Modul zum Exportieren der Zertifikate verwendet haben. Klicken Sie auf 'Weiter'. Wählen Sie nun 'Alle Zertifikate in folgendem Speicher speichern' -> 'auto' und anschließend 'Weiter' -> 'Fertigstellen'. Wenn der Importvorgang erfolgreich war, wird dies durch eine Dialogbox bestätigt. Klicken Sie 'OK'.

Wichtige Zertifikatdaten notieren

Die vorgefertigte IPsec-Beispielkonfiguration enthält normalerweise bereits die korrekte DN der CA ('Aussteller' bzw. 'Issuer').

Klicken Sie nun in der MMC auf 'Datei' -> 'Speichern'. Speichern Sie Ihre Konfiguration mit dem vorgeschlagenen Namen am vorgeschlagenen Ort. Um zu überprüfen, ob die Zertifikat-Daten stimmen, öffnen Sie in der MMC wieder den Ordner 'Eigene Zertifikate' und darin den Ordner 'Zertifikate'. Das Zertifikat für den Client wird angezeigt. Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie aus dem Dropdown-Menü 'Öffnen' und dann den Reiter 'Details'. Wenn Sie auf 'Aussteller' klicken, sehen Sie z.B. Einträge wie die folgenden, die Sie sich notieren müssen:

```
E=bsupport@suse.de
CN=mainca
OU=bu
O=SuSE
L=Nuernberg
S=Franken
C=DE
```

Beenden Sie die Zertifikat-Ansicht mit 'OK' und die MMC mit 'Datei' -> 'Beenden' -> 'Speichern' -> 'Ja'.

IPsec-Verbindung konfigurieren

Installieren Sie das `ipsec.exe` Tool, indem Sie `package.zip` nach `C:\Programme\IPsec\` entpacken. Im nächsten Schritt ersetzen Sie die dort enthaltene Standardversion der Datei `ipsec.conf` durch die exportierte `windows_ipsec.conf` vom VPN-Server (umbenennen). Wechseln Sie dann in das Verzeichnis `C:\Programme\IPsec` und öffnen Sie die Datei mit einem Editor, um die Konfigurationsdaten zu überprüfen. Das folgende Listing gibt die Standardwerte wieder.

```
conn <Name der Verbindung>
        left=%any
        right=<IP des SuSE Linux Standard Servers>
        rightca=<die vorher notierten Werte rückwärts notiert,
                 durch Komma getrennt>
        network=auto
        auto=start
        pfs=yes
```

Die erste Zeile muss unbedingt linksbündig geschrieben werden. Alle anderen Zeilen müssen eingerückt werden. Nachfolgend sehen Sie ein konkretes Beispiel für die `ipsec.conf`:

```
conn me_to_servername
        left=%any
        right=10.10.254.181
        rightca="C=DE,S=Franken,L=Nuernberg,O=SuSE,OU=bu,
                 CN=mainca,E=bsupport@suse.de"
        network=auto
        auto=start
        pfs=yes
```

Erzeugen von Desktop-Links

Abschließend wird der Desktop-Link erzeugt und die Verbindung aktiviert. Legen Sie sich einen Link auf dem Desktop auf die Datei `C:\Programme\IPsec\IPSEC.exe` an. Stellen Sie nun die Verbindung mit dem Internet her und klicken Sie auf den erstellten Link. Ein Fenster öffnet sich, und die IPsec-Filter werden für Ihre aktuelle Verbindung konfiguriert. Testen Sie den Tunnel am besten mit `ping <Client-IP hinter dem Tunnel`. Es erscheint ein- bis zweimal die Meldung „IP-Sicherheit wird verhandelt“, danach sehen Sie die normalen `ping`-Antworten: der Tunnel ist aktiv. Bei Windows 2000 ist erst der zweite Aufruf von `ping` erfolgreich, starten Sie also `ping` erneut.

Verbindung beenden

Um die IPsec-Filter und den Tunnel zu deaktivieren, rufen Sie erst `IPSEC.exe -off` und dann `IPSEC.exe -delete` auf. Auch hierfür empfiehlt es sich, einen Desktop Link anzulegen.

26.3 Masquerading und Firewall

Wird Linux in einer vernetzten Umgebung eingesetzt und muss zwischen verschiedenen internen und externen Bereichen getrennt werden, werden die im Linux-Kernel enthaltenen Funktionen zur Verwaltung von Netzwerkpaketen benutzt. Die Netfilter-Infrastruktur bietet alle Hilfsmittel, um ein Linux-System als wirkungsvolle Firewall zwischen verschiedenen Netzen einzusetzen. Mittels iptables – einer generischen Tabellenstruktur zur Definition von Regelwerken – kann präzise gesteuert werden, welche Pakete des Datenverkehrs passieren dürfen und welche nicht. SuSEfirewall2 und das zugehörige YaST Modul erleichtern Ihnen die Einrichtung eines Paketfilters.

26.3.1 Paketfilterung mit iptables

Netfilter und iptables sind für die Filterung, Veränderung und NAT (*Network Address Translation*) von Netzwerkpaketen zuständig. Filterkriterien und damit verbundene Aktionen werden in Ketten gespeichert und der Reihe nach abgearbeitet, wenn ein Netzwerkpaket eintrifft. Die abzuarbeitenden Regelketten werden in Tabellen gespeichert. Das Kommando `iptables` dient zur Bearbeitung dieser Tabellen und Regelketten.

Linux kennt drei Tabellen für die verschiedenen Funktionen eines Paketfilters:

filter In dieser Tabelle befinden sich die meisten Regeln, da hier das eigentliche *Paketfiltern* stattfindet. Hier finden sich die Regeln für das Annehmen (`ACCEPT`) und Ablehnen (`DROP`) von Paketen.

nat Hier ist die Änderung von Quell- und Zieladressen der Pakete definiert. *Masquerading*, das Sie zum Anbinden eines privaten Kleinnetzes ans Internet verwenden ist ein Spezialfall von NAT.

mangle Mit Hilfe der hier niedergelegten Regeln, können Werte im IP-Header manipuliert werden (zum Beispiel der *Type of Service*).

Es gibt in den genannten Tabellen mehrere vordefinierte Ketten, die die Pakete durchlaufen müssen:

`PREROUTING` Diese Kette ist für Pakete, die gerade am System ankommen.

`INPUT` Diese Kette ist für Pakete, die für systemeigene Prozesse bestimmt sind.

`FORWARD` Diese Kette ist für Pakete bestimmt, die einfach durch das System durchgereicht werden.

`OUTPUT` Diese Kette ist für solche Pakete bestimmt, die im System selbst erzeugt wurden.

`POSTROUTING` Diese Kette ist für alle Pakete, die das System verlassen.

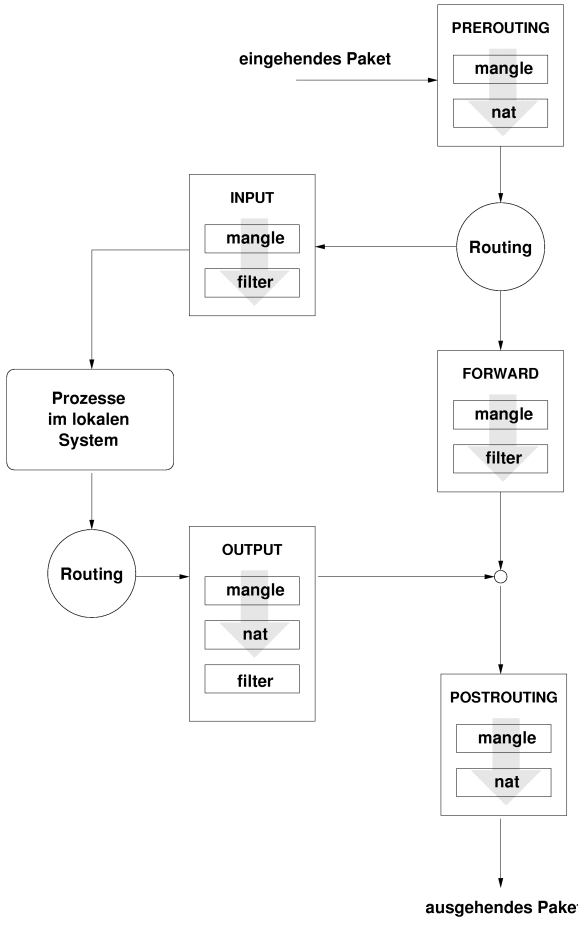

Abbildung 26.7: *iptables: Wege eines Pakets durch das System*

Abbildung 26.7 auf der vorherigen Seite gibt den Weg eines Netzwerkpakets durch das System wieder. Der Darstellbarkeit halber werden die Tabellen nach Ketten gruppiert, obwohl in der Realität die Ketten eigentlich innerhalb der Tabellen organisiert sind.

Im einfachsten Fall trifft auf der `eth0`-Schnittstelle des Systems ein Paket ein, dass für das System selbst bestimmt ist. Zunächst wird dieses Paket in die Kette `PREROUTING` der Tabelle `mangle` geleitet, anschließend wird es in die Kette `PREROUTING` der `nat` Tabelle geleitet. Im angeschlossenen Routingschritt wird festgestellt, dass das Paket für einen Prozess im eigenen System bestimmt ist. Nach Passieren der `INPUT` Ketten in den beiden Tabellen `mangle` und `filter` gelangt das Paket an seinen Bestimmungsort; vorausgesetzt, die Filterregeln in der `filter` Tabelle verhindern dies nicht.

26.3.2 Grundlagen des Masquerading

Masquerading ist der Linux-Spezialfall von NAT (engl. *Network Address Translation*), der Übersetzung von Netzwerkadressen. Zum Einsatz kommt es, wenn ein kleines LAN mit IP-Adressen aus dem privaten Bereich (siehe Abschnitt 21.1.2 auf Seite 459) an das Internet mit seinen offiziellen IP-Adressen angebunden wird. Damit die Rechner im LAN Verbindungen ins Internet aufbauen können, werden die Verbindungen von privaten Adressen auf die offiziellen abgebildet. Dieser Vorgang geschieht auf dem Router, der zwischen LAN und Internet vermittelt. Das Prinzip dahinter ist einfach: Ihr Router hat mehr als ein Netzwerkinterface, typischerweise sind das eine Netzkarte und eine Schnittstelle zum Internet. Eines dieser Interfaces wird Sie nach außen anbinden, eines oder mehrere andere verbinden Ihren Rechner mit den weiteren Rechnern in Ihrem Netz. Sie haben mehrere Rechner im lokalen Netz mit der Netzwerkkarte Ihres Linux-Routers verbunden, die in diesem Beispiel `eth0` heisst. Die Rechner im Netz senden alle Pakete, die nicht für das eigene Netz bestimmt sind, an den Default-Router oder das Default-Gateway.

Hinweis

Einheitliche Netzwerkmasken

Achten Sie beim Konfigurieren Ihres Netzwerks immer auf übereinstimmende broadcast-Adressen und Netzwerkmasken. Andernfalls wird Ihr Netz nicht korrekt arbeiten, da Netzwerkpakete nicht geroutet werden können.

Hinweis

Wird nun einer der Rechner in Ihrem Netz ein Paket fürs Internet abschicken, dann landet es beim Default-Router. Dieser muss so konfiguriert sein, dass er solche Pakete auch weiterleitet. Aus Sicherheitsgründen wird eine SUSE LINUX Installation dies in der Voreinstellung nicht tun! Ändern Sie die Variable `IP_FORWARD` in der Datei `/etc/sysconfig/sysctl` auf `IP_FORWARD=yes`.

Der Zielrechner der Verbindung kennt nur Ihren Router, nicht aber den eigentlichen Absender-Rechner in Ihrem inneren Netzwerk, der hinter Ihrem Router versteckt ist. Daher kommt der Begriff Masquerading. Die Zieladresse für Anwortpakete ist wegen der Adressübersetzung wieder unser Router. Dieser muss die Pakete erkennen und die Zieladresse so umschreiben, dass sie zum richtigen Rechner im lokalen Netz gelangen.

Da der Weg der Pakete von außen nach innen von der Masquerading-Tabelle abhängt, gibt es keine Möglichkeit, von außen eine Verbindung nach innen zu öffnen. Für diese Verbindung gäbe es keinen Eintrag in der Tabelle. Eine etablierte Verbindung hat darüber hinaus in der Tabelle einen zugeordneten Status, so dass dieser Tabelleneintrag nicht von einer zweiten Verbindung genutzt werden kann.

In der Folge ergeben sich nun Probleme mit manchen Anwendungen, zum Beispiel ICQ, cucme, IRC (DCC, CTCP) und FTP (im PORT-Mode). Netscape, das Standard-FTP-Programm und viele andere benutzen den PASSV-Modus, der im Zusammenhang mit Paketfiltern und Masquerading weit weniger problembehaftet ist.

26.3.3 Grundlagen Firewalling

Firewall ist wohl der am weitesten verbreitete Begriff für einen Mechanismus, der zwei Netze miteinander verbindet, aber für möglichst kontrollierten Datenverkehr sorgt. Der Typ Firewall, den wir hier vorstellen, müsste sich eigentlich genauer Paketfilter nennen. Ein Paketfilter regelt den Durchlass anhand von Kriterien wie Protokoll, Port und IP-Adresse. Auf diese Weise können Sie also Pakete abfangen, die aufgrund ihrer Adressierung nicht in Ihr Netz durchdringen sollen. Wenn Sie beispielsweise Zugriffe auf Ihren Webserver zulassen wollen, müssen Sie den dazugehörigen Port freischalten. Der Inhalt dieser Pakete, falls sie legitim adressiert sind (also beispielsweise mit Ihrem Webserver als Ziel), wird nicht untersucht. Das Paket könnte insofern einen Angriff auf ein CGI-Programm auf Ihrem Webserver enthalten und wird vom Paketfilter durchgelassen.

Ein wirksameres — wenn auch komplexeres — Konstrukt ist die Kombination von mehreren Bauarten, beispielsweise ein Paketfilter mit zusätzlichem Application Gateway/Proxy. Der Paketfilter wehrt Pakete ab, die

zum Beispiel an nicht freigeschaltete Ports gerichtet sind. Nur Pakete für ein Application Gateway sollen durchgelassen werden. Dieses Proxy tut nun so, als wäre es der eigentliche Kommunikationspartner des Servers, der mit uns eine Verbindung herstellt. In diesem Sinne kann ein solches Proxy als eine Masquerading-Maschine auf der Ebene des Protokolls der jeweiligen Anwendung angesehen werden. Ein Beispiel für solch ein Proxy ist Squid, ein HTTP Proxy Server, für den Sie Ihren Browser so konfigurieren müssen, dass Anfragen für HTML-Seiten zuerst an den Speicher des Proxy gehen und nur, wenn dort die Seite nicht zu finden ist, vom Proxy in das Internet geschickt werden. Die SUSE proxy-suite (das `proxy-suite`) enthält übrigens einen Proxy-Server für das FTP-Protokoll.

Im Folgenden wollen wir uns auf das Paketfilter-Paket bei SUSE LINUX konzentrieren. Für mehr Informationen und weitere Links zum Thema Firewall lesen Sie bitte das Firewall-HOWTO, enthalten im `howto`. Es lässt sich mit dem Kommando `less /usr/share/doc/howto/en/Firewall-HOWTO.gz` lesen, wenn das Paket `howto` installiert ist.

26.3.4 SuSEfirewall2

SuSEfirewall2 ist ein Skript, das die in `/etc/sysconfig/SuSEfirewall2` konfigurierten Variablen in ein iptables Regelwerk umsetzt.

SuSEfirewall2 kennt drei Sicherheitszonen (von denen allerdings nur die ersten beiden in der nachfolgenden Beispielkonfiguration berücksichtigt werden):

Externes Netz Der Rechner muss vor dem externen Netz geschützt werden, da dieses nicht unter der eigenen Kontrolle steht. Üblicherweise meint man hier das Internet, es können aber ebensogut andere ungeschützte Netze gemeint sein (z.B. WLAN).

Internes Netz Hier ist das eigene Netz, meist das LAN gemeint. Wenn innerhalb dieses Netzwerks IP-Adressen aus dem privaten Bereich verwendet werden (siehe Abschnitt 21.1.2 auf Seite 459), muss Network Address Translation (NAT) durchgeführt werden, damit vom internen Netz auf das externe zugegriffen werden kann.

Demilitarisierte Zone (DMZ) Die hier stehenden Rechner sind sowohl aus dem externen als auch dem internen Netz erreichbar, haben jedoch keinen Zugriff auf das Intranet. Diese Art der Konfiguration

sichert das interne Netz zusätzlich vor dem externen Netz, da von DMZ-Rechnern keine Zugriffsmöglichkeit auf interne Rechner verfügbar ist.

Jeder Netzwerkverkehr, der nicht explizit mit dem Regelwerk erlaubt wurde, wird von iptables unterbunden. Deshalb muss jede einzelne Schnittstelle , über die Pakete ins Netz gelangen, einer der drei Zonen zugeordnet werden und für jede einzelne Zone definiert werden, welche Dienste oder Protokolle erlaubt werden sollen. Das Regelwerk greift allerdings nur für extern erzeugte Pakete. Lokal erzeugte Pakete können immer gesendet werden.

Die Konfiguration lässt sich entweder mit YaST vornehmen (s. Abschnitt 26.3.4 auf Seite 713) oder kann direkt in der Datei `/etc/sysconfig/SuSEfirewall2` erfolgen, die ausführliche englische Kommentare enthält.

Manuelle Konfiguration

Wir werden Ihnen nun Schritt für Schritt eine erfolgreiche Konfiguration vorführen. Es ist bei jedem Punkt angeführt, ob er für Masquerading oder Firewall gilt. In der Konfigurationsdatei ist auch von einer DMZ („Demilitarisierte Zone“) die Rede, auf die an dieser Stelle nicht näher eingegangen wird, da sie ausschließlich in komplexen Netzwerkszenarien größerer Institutionen (Firmen etc.) zum Einsatz kommt und vom Verständnis und dem Konfigurationsaufwand her sehr anspruchsvoll ist.

Aktivieren Sie zunächst mit dem YaST Runlevel Editor die SuSEfirewall2 für Ihren Runlevel (wahrscheinlich 3 oder 5). Dadurch werden symbolische Links für die SuSEfirewall2_* Skripte in den Verzeichnissen `/etc/init.d/rc?.d/` angelegt.

`FW_DEV_EXT` (Firewall, Masquerading)
: die Schnittstelle, die ins Internet führt. Für Modem und DSL verwenden Sie entsprechend `ppp0`, für ISDN `ippp0` und mit `auto` verwenden Sie das Interface der Defaultroute.

`FW_DEV_INT` (Firewall, Masquerading)
: Geben Sie hier die Schnittstelle an, die ins innere, „private“ Netz zeigt (beispielsweise `eth0`). Falls kein inneres Netz vorhanden ist, einfach leer lassen.

`FW_ROUTE` (Firewall, Masquerading)
: Wenn Sie Masquerading brauchen, müssen Sie hier auf jeden Fall `yes`

eintragen. Ihre internen Rechner sind nicht von außen sichtbar, da diese private Netzwerkadressen (zum Beispiel `192.168.x.x`) haben, die im Internet gar nicht geroutet werden.

Bei einer Firewall ohne Masquerading wählen Sie hier nur dann `yes`, wenn Sie Zugang zum internen Netz erlauben wollen. Dazu müssen die internen Rechner offiziell zugewiesene IP-Adressen haben. Im Normalfall sollten Sie allerdings den Zugang von außen auf die internen Rechner *nicht* erlauben!

`FW_MASQUERADE` (Masquerading) Wenn Sie Masquerading brauchen, müssen Sie hier `yes` eintragen. Beachten Sie, dass es sicherer ist, wenn die Rechner des internen Netzes über Proxy-Server auf das Internet zugreifen.

`FW_MASQ_NETS` (Masquerading) Tragen Sie hier die Rechner oder Netzwerke ein, für die Masquerading vorgenommen werden soll. Trennen Sie die einzelnen Einträge durch Leerzeichen. Zum Beispiel:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

`FW_PROTECT_FROM_INTERNAL` (Firewall)
Tragen Sie hier `yes` ein, wenn Sie den Firewall-Rechner auch durch Angriffe vom inneren Netz schützen wollen. Dann müssen Sie die Services, die für das innere Netz verfügbar sind, explizit freigeben. Siehe auch `FW_SERVICES_INT_TCP` und `FW_SERVICES_INT_UDP`.

`FW_AUTOPROTECT_SERVICES` (Firewall)
Im Normalfall auf `yes` lassen, um automatisch explizite Regeln für die laufenden Dienste erzeugen zu lassen.

`FW_SERVICES_EXT_TCP` (Firewall)
Tragen Sie hier die TCP-Ports ein, auf die zugegriffen werden soll. Für einen einfachen Arbeitsplatz zu Hause, der keine Dienste anbieten soll, tragen Sie meist nichts ein.

`FW_SERVICES_EXT_UDP` (Firewall)
Wenn Sie nicht gerade einen Nameserver betreiben, auf den von außen zugegriffen werden soll, lassen Sie dieses Feld leer. Ansonsten fügen Sie hier die benötigten UDP-Ports ein.

`FW_SERVICES_INT_TCP` (Firewall)
Hier werden die für das innere Netz zur Verfügung stehenden Dienste festgelegt. Die Angaben sind analog zu denen unter `FW_SERVICES_EXT_TCP`, beziehen sich hier aber auf das *interne* Netz.

Diese Variable muss lediglich dann konfiguriert werden, wenn `FW_PROTECT_FROM_INTERNAL` aktiviert wurde.

`FW_SERVICES_INT_UDP` (Firewall)
Siehe oben.

`FW_STOP_KEEP_ROUTING_STATE`(Firewall)
Falls Sie automatisch per diald oder über ISDN (dial on demand) ins Internet gehen, so tragen Sie hier `yes` ein.

Damit ist die Konfiguration abgeschlossen. Vergessen Sie nicht, die Firewall zu testen. Rufen Sie als Benutzer `root` `SuSEfirewall2 start` auf, um die Regeln zu erzeugen. Mit beispielsweise einem `telnet` von aussen, sehen Sie, ob diese Verbindung auch tatsächlich abgelehnt wird; Sie sollten dann in `/var/log/messages` in etwa folgende Einträge sehen:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0 OUT=
MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF
PROTO=TCP SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0 OPT
(020405B40402080A061AFEBC0000000001030300)
```

Konfiguration mit YaST

Die grafisch geführte Konfiguration mit YaST erreichen Sie über das YaST-Kontrollzentrum. Wählen Sie aus der Kategorie 'Sicherheit und Benutzer' den Unterpunkt 'Firewall'. Die Konfiguration ist in vier Teilabschnitte gegliedert:

Grundeinstellungen Legen Sie die abzusichernden Interfaces fest. Ist ein einzelner Rechner ohne internes Netz dahinter abzusichern, geben Sie nur die nach außen ins Internet gerichtete Schnittstelle an. Ist ein internes Netz hinter Ihrem System geschaltet, muss auch die nach innen gerichtete Schnittstelle angegeben werden. Verlassen Sie diesen Dialog mit 'Weiter'.

Dienste Diese Option ist nur relevant, falls Sie über Ihr System Dienste anbieten wollen, die vom Internet aus verfügbar sein sollen (Web-Server, Mail-Server etc.). Aktivieren Sie die entsprechenden Checkboxen und/oder nehmen Sie über den Button 'Experten ...' die Freischaltung bestimmter Dienste über deren Portnummern (nachzulesen in `/etc/services`) vor. Soll Ihr Rechner nicht als Server betrieben werden, verlassen Sie diesen Dialog ohne jegliche Änderung mit 'Weiter'.

Features Hier selektieren Sie die wichtigsten Features, die Ihre Firewall auszeichnen sollen:

'Daten weiterleiten und Masquerading durchführen'
Mit dieser Option schirmt Rechner aus dem internen Netz gegen das Internet ab — alle Internetdienste werden scheinbar von Ihrer Firewall benutzt, während die internen Rechner unsichtbar bleiben.

'Vor internem Netz schützen' Nur die freigegebenen Dienste der Firewall sind für die *internen* Rechner verfügbar. Da hier keine Freigabe von Diensten möglich ist, sollten Sie diese Option besser deaktivieren, wenn Sie Zugriff aus dem internen Netz wünschen.

'Alle laufenden Dienste schützen'
Diese Option bedeutet, dass jeglicher externer Netzwerkzugriff auf TCP- und UDP-Dienste der Firewall verhindert wird. Ausgenommen hiervon sind die Dienste, die Sie im vorhergehenden Schritt explizit freigeschaltet haben.

'Traceroute erlauben' Diese Option hilft, das Routing zu Ihrer Firewall hin zu überprüfen.

'IPsec-Pakettransfer als intern behandeln'
Verschlüsselte IPsec-Pakete, die erfolgreich entschlüsselt wurden, werden genauso behandelt wie Pakete, die von Ihrem internen Netzwerk stammen.

Ist die Featurekonfiguration abgeschlossen, verlassen Sie diese Maske mit 'Weiter'.

Protokollierung Hier legen Sie den Umfang der Protokollierung Ihrer Firewall fest. Bevor Sie die 'Optionen zur Fehlersuche' aktivieren, bedenken Sie, dass diese Logfiles sehr große Ausgabemengen erzeugen. Mit der Konfiguration der Protokollierung ist die Konfiguration Ihrer Firewall abgeschlossen. Verlassen Sie den Dialog mit 'Weiter' und bestätigen Sie die nun erscheinende Meldung zur Aktivierung der Firewall.

26.3.5 Weitere Informationen

Aktuelle und für das Paket `SuSEfirewall2` relevante Dokumentation finden Sie unter `/usr/share/doc/packages/SuSEfirewall2`.

Folgende Bücher, Artikel und Webseiten helfen Ihnen beim Verständnis von iptables und netfilter:

Das Firewall-Buch Barth, Wolfgang: *Das Firewall-Buch* 2., überarbeitete Auflage SUSEPRESS, 2003 - (ISBN 3-899900-44-8)

`http://www.netfilter.org` Die Homepage des netfilter/iptables Projekts. Hier steht eine Fülle von Dokumentationen in vielen Sprachen bereit.

26.4 SSH – secure shell, die sichere Alternative

Vernetztes Arbeiten erfordert oft auch den Zugriff auf entfernte Systeme. Hierbei muss sich der Benutzer über sein Login und ein Passwort authentifizieren. Unverschlüsselt im Klartext versandt, könnten diese sensiblen Daten jederzeit von Dritten mitgeschnitten und in ihrem Sinne eingesetzt werden, um zum Beispiel den Zugang des Benutzers ohne sein Wissen nutzen. Abgesehen davon, dass die Angreifer so sämtliche privaten Daten des Benutzers einsehen können, können sie den erworbenen Zugang nutzen, um von dort aus andere Systeme anzugreifen, oder Administrator- bzw. Rootrechte auf dem betreffenden System zu erlangen. Früher wurde zur Verbindungsaufnahme zwischen zwei entfernten Rechnern Telnet verwendet, das keinerlei Verschlüsselungs- oder Sicherheitsmechanismen gegen ein Abhören der Verbindungen vorsieht. Ebensowenig geschützt sind einfache FTP- oder Kopierverbindungen zwischen entfernten Rechnern.

Die SSH-Software liefert den gewünschten Schutz. Die komplette Authentifizierung, in der Regel Benutzername und Passwort, und Kommunikation erfolgen hier verschlüsselt. Zwar ist auch hier weiterhin das Mitschneiden der übertragenen Daten möglich, doch kann der Inhalt mangels Schlüssel durch einen Dritten nicht wieder entschlüsselt werden. So wird sichere Kommunikation über unsichere Netze wie das Internet möglich. SUSE LINUX bietet das Paket OpenSSH an.

26.4.1 Das OpenSSH-Paket

Per Default wird unter SUSE LINUX das Paket OpenSSH installiert. Es stehen Ihnen daher die Programme ssh, scp und sftp als Alternative für telnet, rlogin, rsh, rcp und ftp zur Verfügung.

26.4.2 Das ssh-Programm

Mit ssh können Sie Verbindung zu einem entfernten System aufnehmen und dort interaktiv arbeiten. Es ist somit gleichermaßen ein Ersatz für telnet und rlogin. Aufgrund der Verwandtschaft zu rlogin zeigt der zusätzliche symbolische Name slogin ebenfalls auf ssh. Zum Beispiel kann man sich mit dem Befehl `ssh sun` auf dem Rechner sun anmelden. Anschließend wird man nach seinem Passwort auf dem System sun gefragt.

Nach erfolgreicher Authentifizierung kann dort auf der Kommandozeile oder interaktiv, zum Beispiel mit YaST, gearbeitet werden. Sollten sich der lokale Benutzername und der auf dem entfernten System unterscheiden, kann ein abweichender Name angegeben werden, zum Beispiel `ssh -l august sun` oder `ssh august@sun`.

Darüber hinaus bietet ssh die von rsh bekannte Möglichkeit, Kommandos auf einem anderen System auszuführen. Im nachfolgenden Beispiel wird das Kommando `uptime` auf dem Rechner sun ausgeführt und ein Verzeichnis mit dem Namen `tmp` angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Rechners earth.

```
ssh sonne "uptime; mkdir tmp"
tux@sonne's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Anführungszeichen sind hier zum Zusammenfassen der beiden Anweisungen in einem Kommando erforderlich. Nur so wird auch der zweite Befehl auf dem Rechner sun ausgeführt.

26.4.3 scp – sicheres Kopieren

Mittels scp kopieren Sie Dateien auf einen entfernten Rechner. scp ist der sichere, verschlüsselte Ersatz für rcp. Zum Beispiel kopiert `scp MeinBrief.tex sun:` die Datei `MeinBrief.tex` vom Rechner earth auf den Rechner sun. Insoweit sich die beteiligten Nutzernamen auf earth und sun unterscheiden, geben Sie bei scp die Schreibweise `Nutzername@Rechnername` an. Eine Option `-l` existiert nicht.

Nachdem das Passwort eingegeben wurde, beginnt scp mit der Datenübertragung und zeigt dabei den Fortschritt anhand eines von links nach rechts anwachsenden Balkens aus Sternen an. Zudem wird am rechten Rand die geschätzte Restübertragungszeit (engl. *estimated time of arrival*) angezeigt. Jegliche Ausgabe kann durch die Option `-q` unterdrückt werden.

scp bietet neben dem Kopieren einzelner Dateien ein rekursives Verfahren zum Übertragen ganzer Verzeichnisse: `scp -r src/ sun:backup/` kopiert den kompletten Inhalt des Verzeichnisses `src/` inklusive aller Unterverzeichnisse auf den Rechner sun und dort in das Unterverzeichnis `backup/`. Dieses wird automatisch angelegt wenn es fehlt.

Mittels der Option `-p` kann scp die Zeitstempel der Dateien erhalten. `-C` sorgt für eine komprimierte Übertragung. Dadurch wird einerseits das zu übertragende Datenvolumen minimiert, andererseits aber ein höherer Rechenaufwand erforderlich.

26.4.4 sftp - sicherere Dateiübertragung

Alternativ kann man zur sicheren Datenübertragung sftp verwenden. sftp bietet innerhalb der Sitzung viele der von ftp bekannten Kommandos. Gegenüber scp mag es vor allem beim Übertragen von Daten, deren Dateinamen unbekannt sind, von Vorteil sein.

26.4.5 Der SSH Daemon (sshd) – die Serverseite

Damit ssh und scp, die Clientprogramme des SSH-Paketes, eingesetzt werden können, muss im Hintergrund der SSH-Daemon, ein Server, laufen. Dieser erwartet seine Verbindungen auf `TCP/IP Port 22`.

Während des ersten Starts generiert der Daemon drei Schlüsselpaare. Die Schlüsselpaare bestehen aus einem privaten und einem öffentlichen (engl. *public*) Teil. Deshalb bezeichnet man dies als ein public-key basiertes Verfahren. Um die Sicherheit der Kommunikation mittels SSH zu gewährleisten, darf ausschließlich der Systemadministrator die Dateien der privaten Schlüssel einsehen können. Die Dateirechte werden per Voreinstellung entsprechend restriktiv gesetzt. Die privaten Schlüssel werden lediglich lokal vom SSH-Daemon benötigt und dürfen an niemanden weitergegeben werden. Demgegenüber werden die öffentlichen Schlüsselbestandteile (an der Namensendung `.pub` erkennbar) an Kommunikationspartner weitergegeben und sind entsprechend für alle Benutzer lesbar.

Eine Verbindung wird vom SSH-Client eingeleitet. Der wartende SSH-Daemon und der anfragende SSH-Client tauschen Identifikationsdaten aus, um die Protokoll- und Softwareversion abzugleichen und die Verbindung zu einem falschen Port auszuschließen. Da ein Kindprozess des ursprünglichen SSH-Daemons antwortet, sind gleichzeitig viele SSH-Verbindungen möglich.

OpenSSH unterstützt zur Kommunikation zwischen SSH-Server und SSH-Client das SSH-Protokoll in den Versionen 1 und 2. Nach einer Neuinstallation von SUSE LINUX wird automatisch die aktuelle Protokoll-Version 2 eingesetzt. Möchten Sie nach einem Update weiterhin SSH 1 beibehalten, folgen Sie den Anweisungen in `/usr/share/doc/packages/openssh/README.SuSE`. Dort ist ebenfalls beschrieben, wie Sie in wenigen Schritten eine SSH 1-Umgebung in eine funktionierende SSH 2-Umgebung umwandeln.

Bei Verwendung der SSH Protokoll-Version 1 sendet der Server sodann seinen öffentlichen `host key` und einen stündlich vom SSH-Daemon neu generierten `server key`. Mittels beider verschlüsselt (engl. *encrypt*) der SSH-Client einen von ihm frei gewählten Sitzungsschlüssel (engl. *session key*) und sendet ihn an den SSH-Server. Er teilt dem Server zudem die gewählte Verschlüsselungsmethode (engl. *cipher*) mit.

Die SSH Protokoll-Version 2 kommt ohne den `server key` aus. Stattdessen wird ein Algorithmus nach Diffie-Hellman verwendet, um die Schlüssel auszutauschen.

Die zur Entschlüsselung des Sitzungsschlüssels zwingend erforderlichen privaten host und server keys, können nicht aus den öffentlichen Teilen abgeleitet werden. Somit kann allein der kontaktierte SSH-Daemon mit seinen privaten Schlüsseln den Sitzungsschlüssel entziffern (vgl. `man /usr/share/doc/packages/openssh/RFC.nroff`). Diese einleitende Phase der Verbindung kann man mittels der Fehlersuchoption `-v` des SSH-Clientprogramms gut nachvollziehen. Per Default wird SSH Protokoll-Version 2 verwendet, man kann jedoch mit dem Parameter `-1` auch die SSH Protokoll-Version 1 erzwingen. Indem der Client alle öffentlichen host keys nach der ersten Kontaktaufnahme in `~/.ssh/known_hosts` ablegt, können so genannte man-in-the-middle Angriffe unterbunden werden. SSH-Server, die versuchen, Name und IP-Adresse eines anderen vorzutäuschen, werden durch einen deutlichen Hinweis enttarnt. Sie fallen entweder durch einen gegenüber `~/.ssh/known_hosts` abweichenden host-Schlüssel auf, oder können mangels passendem privaten Gegenstück den vereinbarten Sitzungsschlüssel nicht entschlüsseln.

Es empfiehlt sich, die in `/etc/ssh/` abgelegten privaten und öffentlichen Schlüssel extern und gut geschützt zu archivieren. So können Änderungen der Schlüssel festgestellt und nach einer Neuinstallation die alten wieder eingespielt werden. Dies erspart den Benutzern die beunruhigende Warnung. Ist es sichergestellt, dass es sich trotz der Warnung um den korrekten SSH-Server handelt, muss der vorhandene Eintrag zu diesem System aus `~/.ssh/known_hosts` entfernt werden.

26.4.6 SSH-Authentifizierungsmechanismen

Jetzt erfolgt die eigentliche Authentifizierung, die in ihrer einfachsten Weise aus der Eingabe eines Passwortes besteht, wie es in den oben aufgezeigten Beispielen erfolgte. Ziel von SSH war die Einführung einer sicheren, aber zugleich einfach zu nutzenden Software. Wie bei den abzulösenden Programmen rsh und rlogin muss deshalb auch SSH eine im Alltag einfach zu nutzende Authentifizierungsmethode bieten. SSH realisiert dies mittels eines weiteren hier vom Nutzer erzeugten Schlüsselpaares. Dazu liefert das SSH-Paket das Hilfsprogramm ssh-keygen mit. Nach der Eingabe von `ssh-keygen -t rsa` oder `ssh-keygen -t dsa` wird das Schlüsselpaar generiert und der Basisdateiname zur Ablage der Schlüssel erfragt:

```
Enter file in which to save the key (/home/tux/.ssh/id_rsa):
```

Bestätigen Sie die Voreinstellung und beantworten Sie die Frage nach einer Passphrase. Auch wenn die Software eine leere Passphrase nahelegt, sollte bei der hier vorgeschlagenen Vorgehensweise ein Text von zehn bis 30 Zeichen Länge gewählt werden. Verwenden Sie möglichst keine kurzen und einfachen Worte oder Sätze. Nach erfolgter Eingabe wird zur Bestätigung eine Wiederholung der Eingabe verlangt. Anschließend wird der Ablageort des privaten und öffentlichen Schlüssels, in unserem Beispiel der Dateien `id_rsa` und `id_rsa.pub`, ausgegeben.

```
Enter same passphrase again:
Your identification has been saved in /home/tux/.ssh/id_rsa
Your public key has been saved in /home/tux/.ssh/id_rsa.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@sun
```

Verwenden Sie `ssh-keygen -p -t rsa` bzw. `ssh-keygen -p -t dsa`, um Ihre alte Passphrase zu ändern. Kopieren Sie den öffentlichen Teil des Schlüssels (in unserem Beispiel `id_rsa.pub`) auf den entfernten Rechner und legen Sie ihn dort als `~/.ssh/authorized_keys` ab. Zur Authentifizierung werden Sie beim nächsten Verbindungsaufbau nach Ihrer Passphrase gefragt. Sollte dies nicht der Fall sein, überprüfen Sie bitte Ort und Inhalt der zuvor erwähnten Dateien.

Auf Dauer ist diese Vorgehensweise mühsamer, als die Eingabe eines Passwortes. Entsprechend liefert das SSH-Paket ein weiteres Hilfsprogramm, den ssh-agent, der für die Dauer einer X-session private Schlüssel bereit hält. Dazu wird das gesamte X als Kindprozess des ssh-agents gestartet. Sie erreichen dies am einfachsten, indem Sie am Anfang der Datei

`.xsession` die Variable `usessh` auf `yes` setzen und sich über einen Displaymanager, zum Beispiel KDM oder XDM, anmelden. Alternativ können Sie `ssh-agent startx` verwenden.

Nun können Sie wie gewohnt ssh oder scp nutzen. Insoweit Sie Ihren öffentlichen Schlüssel wie zuvor verteilt haben, sollten Sie jetzt nicht mehr nach dem Passwort gefragt werden. Achten Sie beim Verlassen Ihres Rechners darauf, dass Sie Ihre X-session beenden oder mittels einer passwortgeschützten Bildschirmsperre, zum Beispiel xlock, verriegeln.

Alle wichtigen Änderungen die sich mit der Einführung von SSH Protokoll-Version 2 ergeben haben, wurden auch in der Datei `/usr/share/doc/packages/openssh/README.SuSE` noch einmal dokumentiert.

26.4.7 X-, Authentifizierungs- und sonstige Weiterleitung

Über die bisher beschriebenen sicherheitsrelevanten Verbesserungen hinaus erleichtert ssh auch die Verwendung von entfernten X-Anwendungen. Insoweit Sie `ssh` mit der Option `-X` aufrufen, wird auf dem entfernten System automatisch die DISPLAY-Variable gesetzt und alle X-Ausgaben werden durch die bestehende ssh-Verbindung auf den Ausgangsrechner weitergeleitet. Diese bequeme Funktion unterbindet gleichzeitig die bisher bestehenden Abhörmöglichkeiten bei entfernt aufgerufenen und lokal betrachteten X-Anwendungen.

Durch die gesetzte Option `-A` wird der Mechanismus zur Authentifizierung des ssh-agent auf den nächsten Rechner mit übernommen. Man kann so von einem Rechner zum anderen gehen, ohne ein Passwort eingeben zu müssen. Allerdings nur, wenn man zuvor seinen öffentlichen Schlüssel auf die beteiligten Zielrechner verteilt und korrekt abgelegt hat.

Beide Mechanismen sind vorsichtshalber in der Voreinstellung deaktiviert, können jedoch in der systemweiten Konfigurationsdatei `/etc/ssh/ssh_config` oder der nutzereigenen `~/.ssh/config` permanent eingeschaltet werden.

Man kann ssh auch zur beliebigen Umleitung von TCP/IP-Verbindungen benutzen. Als Beispiel sei hier die Weiterleitung des SMTP- und POP3-Ports aufgeführt:

```
ssh -L 25:sun:25 earth
```

Hier wird jede Verbindung zu earth Port 25, SMTP auf den SMTP-Port von sun über den verschlüsselten Kanal weitergeleitet. Dies ist insbesondere

für Nutzer von SMTP-Servern ohne SMTP-AUTH oder POP-before-SMTP-Fähigkeiten von Nutzen. Mail kann so von jedem beliebigen Ort mit Netzanschluss zur Auslieferung durch den heimischen Mailserver übertragen werden. Analog können mit folgendem Befehl alle POP3-Anfragen (Port 110) an earth auf den POP3-Port von sun weitergeleitet werden:

```
ssh -L 110:sun:110 earth
```

Beide Beispiele müssen Sie als Benutzer `root` ausführen, da auf privilegierte, lokale Ports verbunden wird. Bei bestehender SSH-Verbindung wird Mail wie gewohnt als normaler Benutzer versandt und abgeholt. Der SMTP- und POP3-Host muss dabei auf `localhost` konfiguriert werden. Zusätzliche Informationen entnehmen Sie den Manualpages der einzelnen Programme und den Dateien unter `/usr/share/doc/packages/openssh`.

26.5 Netzwerkauthentifizierung — Kerberos

Ein offenes Netzwerk bietet außer den gewöhnlichen Passwortmechanismen — die von Natur aus unsicher sind — keinerlei Möglichkeit, um sicherzustellen, dass ein Arbeitsplatzrechner seine Benutzer eindeutig identifizieren kann. Das bedeutet, dass eine beliebige Person unter der Vorgabe einer anderen Identität dessen E-Mails abholen, auf dessen private Dateien zugreifen oder einen Dienst starten könnte. Ihre Netzwerkumgebung muss daher die folgenden Anforderungen erfüllen, um wirklich sicher zu sein:

- Lassen Sie alle Benutzer für jeden gewünschten Dienst ihre Identität nachweisen und stellen Sie sicher, dass niemand die Identität eines anderen Benutzers annehmen kann.
- Stellen Sie außerdem sicher, dass jeder Netzwerkserver seine Identität nachweist. Falls Sie dies nicht tun, könnte es einem Angreifer gelingen, sich als der von ihnen angefragte Server auszugeben und vertrauliche Informationen abfangen, die Sie dem Server senden. Dieser Vorgang wird als „Mutual Authentication“ (gegenseitige Authentifizierung) bezeichnet, weil sich der Client beim Server und der Server beim Client authentifiziert.

Durch stark verschlüsselte Authentifizierung hilft Ihnen Kerberos, die o. g. Anforderungen zu erfüllen. Die folgenden Abschnitte zeigen Ihnen, wie dies erreicht wird. Bitte beachten Sie, dass hier nur die grundlegende Arbeitsweise von Kerberos dargelegt wird. Ausführlichere technische Anweisungen sind in der mit Ihrer Kerberos-Implementierung mitgelieferten Dokumentation enthalten.

Hinweis

Das ursprüngliche Kerberos wurde am MIT entwickelt. Neben MIT Kerberos existieren noch verschiedene andere Implementierungen von Kerberos. SUSE LINUX enthält eine freie Implementierung von Kerberos 5, das so genannte Heimdal Kerberos 5 von KTH. Da sich der folgende Text auf gemeinsame Eigenschaften aller Implementierungen von Kerberos bezieht, bezeichnen wir das Programm als Kerberos, es sei denn, es handelt sich um spezifische Information über Heimdal.

Hinweis

26.5.1 Kerberos-Terminologie

Bevor wir auf die Einzelheiten von Kerberos eingehen, wollen wir einen Blick auf das folgende Glossar werfen, das Ihnen helfen wird, mit der Kerberos-Terminologie zurechtzukommen.

Credential Benutzer oder Clients müssen Credentials (Berechtigungsnachweise) vorweisen können, die sie berechtigen, Dienste anzufordern. Kerberos kennt zwei Arten von Berechtigungsnachweisen — Tickets und Authenticators.

Ticket Ein Ticket ist ein serverbezogener Berechtigungsnachweis, den ein Client benutzt, um sich bei einem Server zu authentifizieren, von dem er einen Dienst anfordert. Es enthält den Namen des Servers, den Namen des Clients, die Internetadresse des Clients, einen Zeitstempel (engl. *timestamp*), eine Lebensdauer und einen zufällig generierten Session Key. Alle diese Daten werden mit dem Schlüssel des Servers verschlüsselt.

Authenticator In Verbindung mit dem Ticket wird ein Authenticator benutzt, um zu beweisen, dass der Client, der ein Ticket vorlegt, tatsächlich derjenige ist, der er zu sein vorgibt. Ein Authenticator wird

anhand des Namens des Clients, der IP-Adresse des Arbeitsplatzrechners und der aktuellen Uhrzeit am Arbeitsplatzrechner erstellt — verschlüsselt mit dem Session Key, der nur dem Client und dem Server, von dem er einen Dienst anfordert, bekannt ist. Im Gegensatz zu einem Ticket kann ein Authenticator nur einmal benutzt werden. Ein Client kann selbst einen Authenticator erzeugen.

Principal Ein Kerberos-Principal ist eine unverwechselbare Einheit (ein Benutzer oder ein Dienst), der ein Ticket zugewiesen werden kann. Ein Principal setzt sich aus den folgenden Bestandteilen zusammen:

- **Primary** – Der erste Teil des Principals, der im Falle eines Benutzers mit dem Benutzernamen identisch sein kann.
- **Instance** – Optionale Information, die den Primary beschreibt. Diese Zeichenkette ist durch ein / vom Primary getrennt.
- **Realm** – Der Realm legt Ihren Kerberos-Bereich fest. Normalerweise ist Ihr Realm Ihr Domainname in Großbuchstaben.

Mutual Authentication Kerberos sorgt dafür, dass sich sowohl der Client als auch der Server über die Identität der jeweiligen Gegenpartei sicher sein können. Sie teilen sich einen Session Key, mit dem sie sicher kommunizieren können.

Session Key Session Keys (Sitzungsschlüssel) sind temporäre private Schlüssel, die von Kerberos generiert werden. Sie sind dem Client bekannt und werden zur Verschlüsselung der Kommunikation zwischen dem Client und dem Server benutzt, von dem der Client ein Ticket angefordert und bekommen hat.

Replay Fast alle Nachrichten, die in einem Netzwerk versendet werden, können abgehört, entwendet und erneut versendet werden. Im Zusammenhang mit Kerberos könnte dies äußerst gefährlich sein, falls es einem Angreifer gelingen sollte, Ihre Anforderung für einen Dienst abzufangen, die Ihr Ticket und Ihren Authenticator enthält. Er könnte daraufhin versuchen, sie erneut zu versenden („Replay“) und sich als Sie ausgeben. Allerdings implementiert Kerberos verschiedene Mechanismen, um diesem Problem vorzubeugen.

Server oder Service „Service“ (Dienst) wird benutzt, wenn eine bestimmte Aktion durchgeführt werden soll. Der zugrunde liegende Prozess wird als „Server“ bezeichnet.

26.5.2 Wie funktioniert es?

Kerberos wird oft als „Trusted Third Party"-Authentifizierungsdienst bezeichnet. Das heißt, dass sich alle Clients im Hinblick auf die Identität eines anderen Clients auf die Einschätzung von Kerberos verlassen. Kerberos unterhält eine Datenbank über alle Benutzer und ihre privaten Schlüssel.

Um sicherzustellen, dass Kerberos das in ihn gesetzte Vertrauen auch wirklich verdient, müssen Authentifizierungsserver und Ticket-Granting-Server auf einer dedizierten Maschine laufen. Sorgen Sie dafür, dass nur der Administrator physisch und über das Netzwerk Zugang zu dieser Maschine hat und beschränken Sie die (Netzwerk-)Dienste, die auf diesem Server laufen, auf das absolute Minimum — lassen Sie nicht einmal sshd laufen.

Erste Kontaktaufnahme Ihr erster Kontakt mit Kerberos ähnelt dem gewöhnlichen Einloggen an einem normalen Netzwerksystem. Geben Sie Ihren Benutzernamen ein. Diese Information und der Name des Ticket-Granting Services werden dem Authentifizierungsserver (Kerberos) zugesendet. Falls der Authentifizierungsserver von Ihrer Existenz weiß, generiert er einen (zufälligen) Session Key für den weiteren Gebrauch zwischen Ihrem Client und dem Ticket-Granting Server. Nun wird der Authentifizierungsserver ein Ticket für den Ticket-Granting Server erstellen. Das Ticket enthält die folgenden Informationen, die alle mit einem Session Key verschlüsselt sind, den nur der Authentifizierungsserver und der Ticket-Granting Server kennen:

- die Namen des Clients und des Ticket-Granting Servers
- die aktuelle Uhrzeit
- die Lebensdauer, die diesem Ticket zugewiesen wurde
- die IP-Adresse des Clients
- den neu generierten Session Key

Dann wird das Ticket zusammen mit dem Session Key nochmals in verschlüsselter Form dem Client zurückgesendet, jedoch unter Benutzung des privaten Schlüssels des Clients. Dieser private Schlüssel ist nur Kerberos und dem Client bekannt, da er von Ihrem Benutzerpasswort abgeleitet ist. Sobald der Client diese Antwort erhält, werden Sie nach Ihrem Passwort gefragt. Dieses Passwort wird in den Schlüssel konvertiert, welcher das vom Authentifizierungsserver gesendete Paket entschlüsseln kann. Das Paket wird entpackt und das

Passwort und der Schlüssel werden aus dem Arbeitsspeicher des Arbeitsplatzrechners gelöscht. Ihr Arbeitsplatzrechner kann Ihre Identität nachweisen, bis die Lebensdauer des Ticket-Granting Tickets erlischt.

Anforderung eines Dienstes Um von einem beliebigen Server im Netzwerk einen Dienst anfordern zu können, muss die Client-Anwendung dem Server ihre Identität nachweisen. Daher generiert die Anwendung einen so genannten „Authenticator“. Dieser setzt sich aus den folgenden Bestandteilen zusammen:

- dem Principal des Clients
- der IP-Adresse des Clients
- der aktuellen Uhrzeit
- einer Prüfsumme (bestimmt durch den Client)

Alle diese Informationen werden mit dem Session Key, den der Client bereits für diesen speziellen Server empfangen hat, verschlüsselt. Der Authenticator und das Ticket für den Server werden an den Server gesendet. Der Server benutzt seine Kopie des Session Keys, um den Authenticator zu entschlüsseln, der ihm sämtliche benötigte Informationen über den Client liefert, der seinen Dienst anfordert. Diese Informationen können mit denen verglichen werden, die im Ticket enthalten sind. So prüft der Server, ob Ticket und Authenticator vom gleichen Client stammen.

Gäbe es auf der Serverseite keine Sicherheitsmaßnahmen, so wäre diese Stufe das ideale Ziel für Replay-Attacken. Jemand mit schlechten Absichten könnte versuchen, eine vorher aus dem Netz gestohlene Anforderung erneut zu versenden. Um dies zu verhindern, nimmt der Server keine Anforderungen an, die mit einem Zeitstempel und einem Ticket versehen sind, die ihm schon vorher zugesendet worden waren. Außerdem können Anforderungen abgelehnt werden, deren Zeitstempel in Bezug auf den Zeitpunkt, an dem die Anforderung empfangen wurde, zu sehr abweichen (in die Zukunft und in die Vergangenheit).

Gegenseitige Authentifizierung Die Kerberos-Authentifizierung kann in beide Richtungen benutzt werden. Es geht nicht nur darum, ob der Client wirklich derjenige ist, der er zu sein vorgibt; auch der Server sollte in der Lage sein, sich gegenüber dem Client zu authentifizieren, der seinen Dienst anfordert. Daher versendet er selber auch eine Art Authenticator. Er addiert der Prüfsumme, die er im Authenticator des

Clients erhalten hat, eins hinzu und verschlüsselt sie mit dem Session Key, den er mit dem Client teilt. Der Client betrachtet diese Antwort als Nachweis für die Echtheit des Servers, wonach die Zusammenarbeit zwischen dem Client und dem Server beginnen kann.

Ticket-Granting — Kontaktaufnahme mit allen Servern
Tickets sind für den Gebrauch für jeweils einen Server bestimmt. Das bedeutet, dass Sie ein neues Ticket brauchen, sobald Sie einen anderen Dienst anfordern. Kerberos implementiert einen Mechanismus zur Beschaffung von Tickets für einzelne Server. Dieser Dienst wird als „Ticket-Granting Service“ (Dienst zur Ausstellung von Tickets) bezeichnet. Der Ticket-Granting Service ist ein Dienst wie jeder andere und unterliegt daher den gleichen Zugriffsprotokollen, die bereits erwähnt wurden. Jedes Mal, wenn eine Anwendung ein Ticket benötigt, das noch nicht angefordert wurde, nimmt sie mit dem Ticket-Granting Server Kontakt auf. Diese Anforderung setzt sich aus den folgenden Bestandteilen zusammen:

- dem angeforderten Principal
- dem Ticket-Granting Ticket
- dem Authenticator

Ähnlich wie bei jedem anderen Server überprüft der Ticket-Granting Server das Ticket-Granting Ticket sowie den Authenticator. Falls sie als gültig anerkannt werden, erstellt der Ticket-Granting Server einen neuen Session Key zur Benutzung durch den ursprünglichen Client und den neuen Server. Dann wird das Ticket für den neuen Server mit den folgenden Informationen erstellt:

- dem Principal des Clients
- dem Principal des Servers
- der aktuellen Uhrzeit
- der IP-Adresse des Clients
- dem neu generierten Session Key

Dem neuen Ticket wird eine Lebensdauer zugewiesen, die der verbleibenden Lebensdauer des Ticket-Granting Tickets oder dem Standardwert für den Dienst entspricht, je nachdem, was kürzer ist. Dieses Ticket und der Session Key werden dem Client vom Ticket-Granting Service zugesendet. Dieses Mal ist die Antwort jedoch mit

dem Session Key verschlüsselt, der mit dem ursprünglichen Ticket-Granting Ticket empfangen wurde. Wenn ein neuer Dienst angefordert wird, kann der Client nun die Antwort entschlüsseln, ohne das Benutzerpasswort erneut anzufordern. So kann Kerberos für den Client ein Ticket nach dem anderen erlangen, ohne den Benutzer mehr als einmal beim Login zu belästigen.

Kompatibilität mit Windows 2000 Windows 2000 enthält eine Microsoft-Implementierung von Kerberos 5. Da SUSE LINUX die Heimdal-Implementierung von Kerberos 5 benutzt, werden Sie in der Heimdal-Dokumentation bestimmt einige nützliche Informationen und Anleitungen finden; siehe Abschnitt 26.5.4 auf der nächsten Seite.

26.5.3 Auswirkungen von Kerberos für den Benutzer

Im Idealfall kommt ein Benutzer ausschließlich beim Login an seinem Arbeitsplatzrechner mit Kerberos in Kontakt. Beim Einloggen wird ein Ticket-Granting Ticket erlangt. Beim Ausloggen werden die Kerberos-Tickets des Benutzers automatisch vernichtet, wodurch verhindert wird, dass sich ein anderer Benutzer als dieser spezielle Benutzer ausgibt, wenn dieser nicht eingeloggt ist. Die automatische Vernichtung von Tickets führt zu einer schwierigen Situation, wenn die Sitzung des Benutzers länger dauert als die Höchstlebensdauer, die dem Ticket-Granting Ticket zugewiesen wird (10 Stunden ist ein vernünftiger Wert). Der Benutzer kann sich jedoch ein neues Ticket-Granting Ticket besorgen, indem er kinit startet. Er braucht nur sein Passwort erneut einzugeben — Kerberos wird dafür sorgen, dass er zu jedem gewünschten Dienst Zugang hat, ohne nochmals eine Authentifizierung zu verlangen. Diejenigen, die an einer Liste aller Tickets interessiert sind, die durch Kerberos im Hintergrund für sie erworben wurden, können diese mit klist abrufen.

Es folgt eine Auswahl von Anwendungen, die sich die Kerberos-Authentifizierung zunutze machen. Diese Anwendungen befinden sich unter `/usr/lib/heimdal/bin/`. Sie alle bieten die volle Funktionalität ihrer gewöhnlichen UNIX/Linux-Geschwister sowie den zusätzlichen Vorteil einer transparenten Authentifizierung mit Hilfe von Kerberos:

- telnet/telnetd
- rlogin
- rsh, rcp, rshd

- popper/push
- ftp/ftpd
- su
- imapd
- pine

Wie Sie sehen werden, brauchen Sie Ihr Passwort nicht einzugeben, um diese Anwendungen benutzen zu können, da Kerberos Ihre Identität bereits nachgewiesen hat. ssh — sofern mit Kerberos-Unterstützung kompiliert — kann sogar alle Tickets, die Sie für einen Arbeitsplatzrechner erworben haben, an einen anderen Arbeitsplatz weiterleiten. Wenn Sie ssh benutzen, um sich auf einem anderen Arbeitsplatzrechner einzuloggen, sorgt ssh dafür, dass die verschlüsselten Inhalte der Tickets der neuen Situation angepasst werden. Es ist nicht ausreichend, die Tickets einfach von einem Arbeitsplatzrechner auf einen anderen zu kopieren, da das Ticket spezifische Information über den Arbeitsplatzrechner enthält (die IP-Adresse). XDM und KDM bieten ebenfalls Kerberos-Unterstützung. Lesen Sie im *Kerberos V5 UNIX User's Guide* unter `http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-user.html` mehr über die Kerberos-Netzwerkanwendungen.

26.5.4 Weitere Informationen über Kerberos

SUSE LINUX enthält eine freie Implementierung von Kerberos, die als Heimdal bezeichnet wird. Die entsprechende Dokumentation wird zusammen mit dem Paket `heimdal` unter `/usr/share/doc/packages/heimdal/doc/heimdal.info` installiert. Die Dokumentation ist auch auf der Internetseite des Projekts unter `http://www.pdc.kth.se/heimdal/` erhältlich.

Auf der offiziellen Website der Kerberos-Implementierung des MIT finden Sie Links zu anderen relevanten Ressourcen im Zusammenhang mit Kerberos: `http://web.mit.edu/kerberos/www/`

Ein „klassischer" Dialog, der die Arbeitsweise von Kerberos erläutert. Nicht allzu technisch, aber trotzdem hochinteressant: `http://web.mit.edu/kerberos/www/dialogue.html`

Dieses Papier vermittelt ein umfangreiches Verständnis über die grundlegende Arbeitsweise von Kerberos, ist jedoch nicht übermäßig schwer

zu verstehen. Es bietet außerdem eine Menge Möglichkeiten für weitere Nachforschungen zu Kerberos: `ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS`

Diese Links bieten eine kurze Einführung in Kerberos sowie Antworten auf viele Fragen im Zusammenhang mit der Installation, Konfiguration und Administration von Kerberos: `http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-user.html` `http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-install.html` `http://web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3/doc/krb5-admin.html`

Das offizielle Kerberos-FAQ: `http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html`

Tung, Brian: *Kerberos — A Network Authentication System*. Addison Wesley, 1999. - (ISBN 0-201-37924-4)

26.6 Installation und Administration von Kerberos

Dieser Abschnitt erläutert die Installation des Heimdal Kerberos sowie einige Aspekte der Administration. Es wird vorausgesetzt, dass Sie mit den Grundlagen von Kerberos vertraut sind (siehe auch Abschnitt 26.5 auf Seite 721).

26.6.1 Festlegung der Kerberos-Realms

Die „Domain“ einer Kerberos-Installation wird als Realm bezeichnet und hat einen Namen wie `FOOBAR.COM` oder einfach nur `ACCOUNTING`. Da Kerberos Groß-/Kleinbuchstaben unterscheidet, ist `foobar.com` ein anderer Realm als `FOOBAR.COM`. Die Wahl von Groß-/Kleinbuchstaben ist Ihnen überlassen. Es ist jedoch üblich, für Realm-Namen Großbuchstaben zu benutzen.

Es ist empfehlenswert, Ihren DNS-Domainnamen (oder eine Subdomain wie `ACCOUNTING.FOOBAR.COM`) zu benutzen. Wie Sie später sehen werden, haben Sie es als Administrator viel leichter, wenn Sie Ihre Kerberos-Clients so konfigurieren, dass das KDC und andere Kerberos-Dienste via DNS ansprechbar sind. Um dies zu ermöglichen, ist es sinnvoll, wenn der Realm-Name eine Subdomain Ihres DNS-Domainnamens ist.

Im Gegensatz zum DNS-Namensraum ist Kerberos nicht hierarchisch gegliedert. Sie können nicht einen Realm namens `FOOBAR.COM` aufsetzen, darunter zwei „Subrealms“ namens `DEVELOPMENT` und `ACCOUNTING` erstellen und erwarten, dass die beiden untergeordneten Realms irgendwie Principals von `FOOBAR.COM` übernehmen. Stattdessen hätten Sie drei getrennte Realms, für die Sie „Crossrealm“-Authentifizierung konfigurieren müssten, um Benutzern eines Realms zu ermöglichen, mit Servern oder Benutzern eines anderen Realms zu interagieren. Die Einrichtung der Crossrealm-Authentifizierung wird beispielsweise in [19] beschrieben.

Der Einfachheit halber nehmen wir an, dass Sie für Ihre gesamte Organisation nur einen Realm anlegen. Im restlichen Teil dieses Abschnittes wird der Realm-Name `SAMPLE.COM` für alle Beispiele benutzt.

26.6.2 Einrichtung der KDC-Hardware

Wenn Sie Kerberos benutzen möchten, brauchen Sie zunächst einen Rechner, der als Key Distribution Center (KDC) eingesetzt wird. Auf diesem Rechner befindet sich die gesamte Kerberos-Benutzerdatenbank mit den Passwörtern und allen Informationen.

Das KDC ist der wichtigste Teil Ihrer Sicherheitsinfrastruktur — wenn jemand hier eindringt, sind alle Benutzerkonten und die gesamte Infrastruktur, die durch Kerberos geschützt wird, offengelegt. Ein Angreifer, der Zugang zur Kerberos-Datenbank hat, kann ein beliebiges Principal in der Datenbank verkörpern! Sorgen Sie dafür, dass die Sicherheitsvorkehrungen für diesen Rechner so strikt wie möglich sind:

- Stellen Sie den Server an einem physikalisch sicheren Standort auf, zum Beispiel in einem abgeschlossenen Serverraum, zu dem nur ein begrenzter Personenkreis Zugang hat.
- Lassen Sie außer dem KDC keine anderen Netzwerkanwendungen auf dem Rechner laufen. Dies gilt sowohl für Server- als auch für Clientanwendungen. Das KDC sollte beispielsweise keine Dateisysteme über NFS importieren oder DHCP benutzen, um seine Netzwerkkonfiguration abzurufen.

  Ein guter Ansatz wäre, zunächst nur ein Minimalsystem zu installieren und dann die Liste aller installierten Pakete zu überprüfen und eventuelle unnötige Pakete zu löschen. Dies schließt Server wie inetd, portmap und cups sowie alles ein, was mit X11 zu tun hat. Selbst die Installation eines SSH-Servers stellt ein potentielles Sicherheitsrisiko dar.

Auf diesem Rechner gibt es kein grafisches Login, da auch ein X-Server ein potentielles Sicherheitsrisiko darstellt. Kerberos hat jedoch ein eigenes Administrationsinterface.

- Konfigurieren Sie `/etc/nsswitch.conf` so, dass nur in lokalen Dateien nach Benutzern und Gruppen gesucht wird. Ändern Sie die Zeilen für `passwd` und `group` wie folgt:

  ```
  passwd:         files
  group:          files
  ```

  Editieren Sie die Dateien `passwd`, `group`, `shadow` und in `/etc/` und entfernen Sie die Zeilen, die mit einem Pluszeichen anfangen (diese werden für NIS-Anfragen benutzt).

  Sie sollten sich auch überlegen, DNS-Anfragen zu deaktivieren, da dies einen Risikofaktor darstellt. Falls in der DNS Resolver Library eine Sicherheitslücke ist, könnte ein Angreifer das KDC überlisten, eine DNS-Anfrage durchzuführen, die diese Lücke ausnutzt. Um DNS-Anfragen zu deaktivieren, löschen Sie einfach `/etc/resolv.conf`.

- Deaktivieren Sie alle Benutzerkonten außer dem von Root, indem Sie `/etc/shadow` editieren und die gehashten Passwörter durch Sternchen oder Ausrufezeichen ersetzen.

26.6.3 Zeitsynchronisation

Um Kerberos erfolgreich einsetzen zu können, müssen alle Systemuhren in Ihrer Organisation in einem bestimmten Bereich synchronisiert werden. Der Grund hierfür ist, dass Kerberos versuchen wird, Sie vor erneut versendeten Credentials (Replay) zu schützen. Es könnte einem Angreifer gelingen, Kerberos-Credentials im Netzwerk zu beobachten und diese zu benutzen, um den Server anzugreifen. Kerberos setzt verschiedene Verteidigungsmechanismen ein, um dies zu verhindern. Einer dieser Mechanismen sieht vor, dass die Tickets mit Zeitstempeln versehen werden. Ein Server, der ein Ticket mit einem nicht aktuellen Zeitstempel erhält, wird das Ticket zurückweisen.

Natürlich erlaubt Kerberos beim Vergleichen von Zeitstempeln einen gewissen Spielraum. Computeruhren können jedoch äußerst ungenau sein — es ist nicht ungewöhnlich, das PC-Uhren im Laufe einer Woche eine halbe Stunde vor- oder zurückgehen. Sie sollten daher alle Hosts im Netzwerk so konfigurieren, dass ihre Uhren mit einer zentralen Zeitquelle synchronisiert werden.

Sie können dies sehr einfach bewerkstelligen, indem Sie auf einem Rechner einen NTP-Zeitserver installieren und alle Clients ihre Uhren mit diesem Server synchronisieren lassen. Dies kann erreicht werden, indem Sie einen NTP-Daemon im Client-Modus auf allen Rechnern laufen lassen oder `ntpdate` einmal am Tag von allen Clients ausführen lassen (diese Lösung funktioniert wahrscheinlich nur bei einer kleineren Anzahl von Clients).

Das KDC selber muss auch mit der gemeinsamen Zeitquelle synchronisiert werden. Da ein NTP-Daemon auf diesem Rechner ein Sicherheitsrisiko darstellen würde, ist es wahrscheinlich das Beste, `ntpdate` via einen Croneintrag auszuführen.

Eine Beschreibung der Konfiguration von NTP finden Sie im Abschnitt 21.12 auf Seite 577. Weiterführende Information ist in der NTP-Dokumentation auf Ihrem installierten System unter `/usr/share/doc/packages/xntp-doc` erhältlich.

Selbstverständlich können Sie die maximale Abweichung, die Kerberos bei der Überprüfung von *time stamps* toleriert, nach eigenen Vorstellungen anpassen. Dieser Wert (`clock skew`) wird in der Konfigurationsdatei `krb5.conf` verändert, wie unter Abschnitt 26.6.6 auf Seite 738 beschrieben.

26.6.4 Konfiguration der Protokollfunktion

Standardmäßig protokollieren die auf dem KDC-Host laufenden Kerberos-Daemons ihre Information zum syslog-Daemon. Falls Sie die Aktivitäten Ihres KDC beobachten möchten, ist es vielleicht nützlich, diese Protokolldateien regelmäßig zu verarbeiten und auf ungewöhnliche Ereignisse oder potentielle Probleme zu untersuchen.

Um dies zu erreichen, kann man auf dem KDC-Host ein Protokollscannerskript laufen lassen oder diese Protokolldaten via rsync vom KDC auf einen anderen Host kopieren und die Protokollanalyse dort durchführen. Es wird davon abgeraten, die gesamte Protokollausgabe über die Weiterleitungsfunktion von syslogd weiterzuleiten, da die Information in unverschlüsselter Form im Netzwerk übertragen wird.

26.6.5 Installation des KDC

Dieser Abschnitt erläutert die Erstinstallation des KDC, einschließlich der Einrichtung eines administrativen Principals.

Installation der RPMs

Bevor Sie anfangen können, müssen Sie die Kerberos-Software installieren. Installieren Sie die RPMs `heimdal`, `heimdal-lib` und `heimdal-tools` auf dem KDC:

```
rpm -ivh heimdal-*.rpm heimdal-lib-*.rpm heimdal-tools*.rpm
```

Setzen des Master Keys

Der nächste Schirtt ist die Initialisierung der Datenbank, in der Kerberos sämtliche Informationen über die Principals speichert. Zuerst muss der Master Key der Datenbank gesetzt werden, der benötigt wird, um die Datenbank vor unbeabsichtigter Offenlegung zu schützen, besonders wenn diese auf ein Band gesichert wird.

Der Master Key wird aus einer Passphrase generiert und in einer Datei gespeichert, die als Stash File bezeichnet wird. Daher brauchen Sie nicht jedes Mal, wenn das KDC neu gestartet wird, das Passwort einzugeben. Wählen Sie eine gute Passphrase, beispielsweise einen Satz aus einem Buch, das Sie an einer zufälligen Stelle aufschlagen.

Wenn Sie die Kerberos-Datenbank auf Band sichern (`/var/heimdal/heimdal.db`), sichern Sie bitte nicht die stash Datei (in `/var/heimdal/m-key`). Ansonsten könnte jeder, der das Band lesen kann, die Datenbank entschlüsseln. Aus diesem Grunde ist es empfehlenswert, eine Kopie der Passphrase in einem Safe oder an einem anderen sicheren Ort aufzubewahren, da Sie diese benötigen, wenn Sie nach einem Absturz Ihre Datenbank von Band wiederherstellen.

Um den Master Key zu setzen, starten Sie die Utility kstash ohne zusätzliche Argumente und geben die Passphrase zweimal ein:

```
kstash

Master key:<enter pass phrase>
Verifying password - Master key:<enter pass phrase again>
```

Anlegen des Realms

Zuletzt müssen die Einträge für Ihren Realm in der Kerberos-Datenbank erstellt werden. Starten Sie die Utility kadmin mit der Option `-l`. Diese Option veranlasst kadmin, auf die lokale Datenbank zuzugreifen. Standardmäßig versucht kadmin, den Kerberos-Administrationsdienst über

das Netzwerk zu erreichen. In diesem Stadium würde dies nicht funktionieren, da dieser Dienst noch nicht läuft.

Nun weisen Sie kadmin an, Ihren Realm zu initialisieren. kadmin wird eine Reihe von Fragen stellen. Zunächst ist es das Beste, die von kadmin angebotenen Standardeinstellungen anzunehmen:

```
kadmin -l

kadmin> init SAMPLE.COM
Realm max ticket life [unlimited]: <press return>
Realm max renewable ticket life [unlimited]: <press return>
```

Um zu prüfen, ob etwas geschehen ist, benutzen Sie den Befehl list:

```
kadmin> list *

default@SAMPLE.COM
kadmin/admin@SAMPLE.COM
kadmin/hprop@SAMPLE.COM
kadmin/changepw@SAMPLE.COM
krbtgt/SAMPLE.COM@SAMPLE.COM
changepw/kerberos@SAMPLE.COM
```

Dies zeigt, dass es jetzt in der Datenbank eine Reihe von Principals gibt, die alle für den internen Gebrauch durch Kerberos bestimmt sind.

Erstellung eines Principals

Nun schaffen Sie zwei Kerberos-Principals für sich selbst — ein „normales“ Principal für Ihre tägliche Arbeit und eines für administrative Aufgaben im Zusammenhang mit Kerberos. Verfahren Sie wie folgt, um den Login-Namen `newbie` einzurichten:

```
kadmin -l

kadmin> add newbie
Max ticket life [1 day]: <press return>
Max renewable life [1 week]: <press return>
Principal expiration time [never]: <press return>
Password expiration time [never]: <press return>
Attributes []: <press return>
newbie@SAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Sie können die Standardwerte mit Enter bestätigen. Wählen Sie ein geeignetes Passwort.

Danach erstellen Sie ein anderes Principal namens `newbie/admin` durch Eingabe von `add newbie/admin` am `kadmin`-Prompt. Der Suffix `admin` hinter dem Benutzernamen bezeichnet die „Rolle“ (engl. *role*). Später werden Sie diese administrative Rolle benutzen, um die Kerberos-Datenbank zu administrieren.

Ein Benutzer kann mehrere „Rollen“ haben, die unterschiedlichen Zwecken dienen. Ihre Handhabung hat dennoch nichts mit Magie zu tun — sehen Sie sie einfach als völlig unterschiedliche Accounts mit ähnlichen Namen an.

Starten des KDC

Starten Sie die KDC-Daemons. Dies schließt den eigentlichen kdc (der Daemon, der für die Benutzerauthentifizierung und Ticketanfragen zuständig ist), kadmind (der Server für die Fernadministration) sowie kpasswd (zuständig für Passwortänderungsanfragen von Benutzern) ein. Um den Daemon manuell zu starten, geben Sie Folgendes ein:

```
rckdc start
Starting kdc                done
```

Sorgen Sie dafür, dass das KDC standardmäßig gestartet wird, wenn der Server neu gestartet wird. Dies wird mit Hilfe des Befehls `insserv kdc` bewerkstelligt.

26.6.6 Konfiguration von Kerberos-Clients

Die Konfiguration von Kerberos kann grundsätzlich auf zweierlei Weise erfolgen — über eine statische Konfiguration mit der Datei `/etc/krb5.conf` oder über eine dynamische Konfiguration via DNS. Bei der DNS-Konfiguration versuchen Kerberos-Anwendungen, die KDC-Dienste durch DNS-Einträge zu finden. Bei der statischen Konfiguration müssen Sie die Hostnamen Ihres KDC-Servers in der Datei `krb5.conf` eintragen (und die Datei aktualisieren, wenn das KDC „umzieht“ oder Sie Ihren Realm in irgendeiner anderen Weise neu konfigurieren).

Die DNS-basierte Konfiguration ist gewöhnlich viel flexibler und der Konfigurationsaufwand pro Rechner viel geringer. Dieser Ansatz erfordert jedoch, dass Ihr Realm-Name mit Ihrer DNS-Domain identisch ist oder eine Subdomain hiervon ist.

Außerdem verursacht die Konfiguration von Kerberos via DNS ein kleines Sicherheitsproblem, denn ein Angreifer kann Ihre Infrastruktur durch Ihren DNS erheblich stören (durch Abschuss des Nameservers, Verfälschung von DNS-Einträgen [Spoofing] usw.). Im schlimmsten Fall führt dies jedoch zu einem DoS. Ein ähnliches Szenario kann auch bei der statischen Konfiguration auftreten, es sei denn, Sie geben in `krb5.conf` IP-Adressen anstelle von Hostnamen ein.

Statische Konfiguration

Eine Art der Kerberos-Konfiguration ist der Änderung der Konfigurationsdatei `/etc/krb5.conf`. Die Datei, die standardmäßig im installierten System vorhanden ist, enthält einige Beispieleinträge. Entfernen Sie diese, bevor Sie mit Ihrer eigenen Konfiguration beginnen.

`krb5.conf` besteht aus mehreren Abschnitten. Jeder dieser Abschnitte beginnt mit dem Namen des Abschnitts in eckigen Klammern (`[Beispielname]`).

Für die statische Konfiguration fügen Sie bitte den folgenden Abschnitt in `krb5.conf` ein (wobei `kdc.sample.com` der Hostname des KDCs ist):

```
[libdefaults]
        default_realm = SAMPLE.COM

[realms]
        SAMPLE.COM = {
                kdc = kdc.sample.com
                kpasswd_server = kdc.sample.com
                admin_server = kdc.sample.com
        }
```

Über die Zeile `default_realm` wird die standardmäßige Realm für Kerberos-Applikationen festgelegt.

Falls Sie mehrere Realms haben, fügen Sie einfach dem Abschnitt `[realms]` einen weiteren Ausdruck hinzu.

Fügen Sie dieser Datei auch einen Ausdruck hinzu, der besagt, wie Anwendungen Hostnamen zu Realms zuordnen müssen. Wenn man beispielsweise eine Verbindung zu einem entfernten Host aufbaut, muss die Kerberos-Library wissen, in welchem Realm sich dieser Host befindet. Dies muss im Abschnitt `[domain_realms]` konfiguriert werden:

```
[domain_realm]
        .sample.com = SAMPLE.COM
        www.foobar.com = SAMPLE.COM
```

Dieser Eintrag teilt der Library mit, dass sich alle Hosts in den `sample.com` DNS-Domains in dem Kerberos-Realm `SAMPLE.COM` befinden. Außerdem sollte auch ein externer Host namens `www.foobar.com` als Angehöriger des Realms `SAMPLE.COM` betrachtet werden.

DNS-basierte Konfiguration

Die DNS-basierte Kerberos-Konfiguration macht intensiven Gebrauch von SRV-Einträgen (Siehe *(RFC2052) A DNS RR for specifying the location of services* unter `http://www.ietf.org`). Diese Einträge wurden in früheren Implementierungen des BIND-Nameservers noch nicht unterstützt. Deshalb ist BIND Version 8 (oder spätere Versionen) erforderlich.

Was Kerberos betrifft, ist der Name eines SRV-Eintrags immer wie folgt aufgebaut: `_service._proto.realm`, wobei realm der Kerberos-Realm ist. Beachten Sie, dass DNS bei Domainnamen keine Groß-/Kleinbuchstaben unterscheidet, so dass Kerberos-Realms, die Groß-/Kleinschreibung unterscheiden, bei dieser Konfigurationsmethode nicht mehr funktionieren würden. `_service` ist der Name eines Dienstes (verschiedene Namen werden benutzt, wenn beispielsweise eine Verbindung zum KDC oder zum Passwortdienst aufgebaut wird). `_proto` kann entweder `_udp` oder `_tcp` sein, aber nicht alle Dienste unterstützen beide Protokolle.

Der Datenteil der SRV Resource Records besteht aus einem Prioritätswert, einer Gewichtung, einer Portnummer und einem Hostnamen. Die Priorität definiert die Reihenfolge, in welcher Hosts versucht werden sollen (kleinere Werte stellen eine höhere Priorität dar). Die Gewichtung wird benutzt, um ein gewisses Load-Balancing zwischen Servern gleicher Priorität zu unterstützen. Diese Funktion wird kaum gebraucht, so dass Sie diese auf Null setzen können. Bei der Suche nach Diensten sucht Heimdal Kerberos zur Zeit nach den folgenden Namen:

_kerberos Definiert die Lokalisierung des KDC-Daemons (der Authentifizierungs- und Ticket-Granting-Server). Typischerweise sehen die Einträge wie folgt aus:

```
_kerberos._udp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
_kerberos._tcp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
```

_kpasswd Beschreibt die Lokalisierung des Servers für Passwortänderungen. Typischerweise sehen die Einträge wie folgt aus:

```
_kpasswd._udp.SAMPLE.COM.   IN  SRV    0 0 464 kdc.sample.com.
```

Dakpasswdd TCP nicht unterstützt, sollte es keinen `_tcp` Eintrag geben.

_kerberos-adm Beschreibt die Lokalisierung des Fernadministrationsservers. Typischerweise sehen die Einträge wie folgt aus:

```
_kerberos-adm._tcp.SAMPLE.COM. IN  SRV    0 0 749 kdc.sample.com.
```

Da kadmind UDP nicht unterstützt, sollte es keinen `_udp` Eintrag geben.

Wie bei der statischen Konfigurationsdatei gibt es einen Mechanismus, der Clients darüber informiert, dass ein bestimmter Host sich in dem Realm `SAMPLE.COM` befindet, selbst wenn er kein Teil der DNS-Domain sample.com ist. Dies kann erreicht werden, indem man `_kerberos.hostname` einen TXT-Eintrag hinzufügt:

```
_kerberos.www.foobar.com.  IN  TXT "SAMPLE.COM"
```

Anpassung der Uhrabweichung

Über die Variable `clock skew` setzen Sie die Toleranzgrenzen fest, innerhalb derer Tickets akzeptiert werden, deren Zeitstempel nicht exakt mit der Systemuhr des Hostssystems übereinstimmen.

Im Normalfall ist diese Größe mit 300 Sekunden (5 Minuten) angegeben. Ein Ticket kann also einen Zeitstempel tragen, der fünf Minuten in Vergangenheit oder Zukunft von der Systemzeit des Servers abweicht, um noch akzeptiert zu werden.

Verwenden Sie NTP zur Zeitsynchronisation auf allen Hosts, kann dieser Wert auf eine Minute reduziert werden.

Die `clock skew` Variable passen Sie in `/etc/krb5.conf` wie folgt an:

```
[libdefaults]
        clockskew = 120
```

Der YaST Kerberos-Client

Die Konfiguration eines Kerberos-Clients können Sie alternativ zu der wie oben beschriebenen manuellen Vorgehensweise auch mit YaST vornehmen. Öffnen Sie im YaST Contol Center 'Netzwerkdienste' → 'Kerberos-Client'. Aktivieren Sie in einem nächsten Schritt die Checkbox 'Kerberos

verwenden'. Sollte Ihr Client DNS-basiert konfiguriert werden, können Sie die nun folgenden 'Grundeinstellungen für Kerberos' übernehmen. Wird diese Art der Konfiguration innerhalb Ihrer Domain nicht angeboten, tragen Sie die Werte für 'Standard-Domain', 'Standard-Realm' und die 'KDC-Serveradresse' selbst ein. Über den Button 'Erweiterte Einstellungen' gelangen Sie in eine weitere YaST Maske, in der Sie Feineinstellungen betreffs des Tickets, der OpenSSH-Unterstützung und der Zeitsynchronisation vornehmen können.

Zu den 'Erweiterten Einstellungen' des Kerberos-Clients gehören sämtliche Ticketattribute. Möchten Sie Ihre Tickets nicht nur an dieser einen Maschine nutzen, sondern wünschen eine Weiterleitung Ihrer kompletten Identität, aktivieren Sie die Checkbox 'Tickets sind weiterleitbar (forwardable)'. Sollen lediglich bestimmte Tickets weitergereicht werden, aktivieren Sie 'Tickets sind weitervermittelbar (proxiable)'. 'Tickets behalten' bewirkt, dass ein PAM-Modul das Ticket auch nach Abschluss einer Sitzung behält. Geben Sie die 'Standardlebensdauer' für Ihre Tickets (Einheiten sind *d*, *h* und *m* für Tage, Stunden und Minuten; keine Leerzeichen zwischen Wert und Einheit) an. Wünschen Sie Kerberos-Unterstützung für Ihren OpenSSH-Client, aktivieren Sie die entsprechende Checkbox. Nun werden Kerberos-Tickets für die Authentifizierung am SSH-Server verwendet. Anschließend haben Sie die Möglichkeit über 'Kleinste UID' Benutzer mit einer User-ID kleiner als die angegebene von der Kerberos-Authentifizierung ausschließen. Dies kann z.B. für den Systemadministrator (`root`) Sinn machen. Setzen Sie nun noch die maximale Toleranz zwischen den Zeitstempeln (engl. *time stamps*) und der Systemzeit Ihres Hosts fest. Möchten Sie Ihre Systemzeit mit der des NTP-Servers synchronisieren, konfigurieren Sie Ihr System über den Button 'NTP-Konfiguration' als NTP-Client. Nachdem Sie die Konfiguration abgeschlossen haben, wird YaST automatisch alle Anpassungen vornehmen und Ihr Kerberos-Client ist einsatzbereit.

26.6.7 Einrichtung der Fernadministration

Um der Kerberos-Datenbank Principals hinzufügen bzw. löschen zu können, ohne direkten Zugang zur Konsole des KDC zu haben, teilen Sie dem Kerberos-Adminserver mit, welche Principals hierzu berechtigt sind.

Sie können dies erreichen, indem Sie die Datei `/var/heimdal/kadmind.acl` editieren (ACL ist die Abkürzung von Access Control List). Die ACL-Datei ermöglicht eine Spezifizierung der Vorrechte und die Feineinstellung des Kontrollgrads. Nähere Informationen sind auf der Manpage (`man 8 kadmind`) erhältlich.

Erlauben Sie sich nun, mit der Datenbank alles zu tun, was Sie möchten, indem Sie der Datei die folgende Zeile hinzufügen:

```
newbie/admin all
```

Ersetzen Sie den Benutzernamen `newbie` mit Ihrem eigenen Benutzernamen. Starten Sie nun den KDC neu, um Ihre Änderungen aktiv werden zu lassen.

Fernadministration mittels kadmin

Die Fernadministration von Kerberos sollte nun mit Hilfe des Tools kadmin möglich sein. Zunächst brauchen Sie ein Ticket für Ihr Admin-Principal. Dieses Ticket wird gebraucht, wenn Sie ein Verbindung zum kadmin-Server herstellen:

```
kinit newbie/admin

newbie/admin@SAMPLE.COM's Password: <enter password>

/usr/sbin/kadmin

kadmin> privs
change-password, list, delete, modify, add, get
```

Mit dem Befehl privs können Sie überprüfen, welche Vorrechte Sie haben. Die obige Liste führt sämtliche Vorrechte auf.

Zum Beispiel können Sie das Principal `newbie` modifizieren:

```
kadmin> mod newbie
Max ticket life [1 day]:2 days
Max renewable life [1 week]:
Principal expiration time [never]:2005-01-01
Password expiration time [never]:
Attributes []:
```

Dies ändert die maximale Lebensdauer des Tickets auf zwei Tage und setzt das Auslaufdatum auf den 01.01.2005.

Grundlegende kadmin Kommandos

Hier folgt eine kurze Liste der wichtigsten kadmin Kommandos; bitte konsultieren Sie die Manualpage von `kadmin` für weitergehende Informationen.

add `principal` Fügt ein neues Principal hinzu.

modify `principal` Editieren verschiedener Attribute eines Principals, wie z. B. der maximalen Lebensdauer der Tickets und das Auslaufdatum des Kontos/Accounts.

delete `principal` Entfernt ein Principal aus der Datenbank.

rename `principal neuername` benennt ein Principal in `neuername` um.

list ⟨***pattern***⟩ Listet alle Principals auf, die dem angegebenen Pattern (Muster) entsprechen. Patterns funktionieren ähnlich wie die Shell Globbing Patterns: `list newbie*` würde in unserem Beispiel `newbie` und `newbie/admin` auflisten.

get ⟨***principal***⟩ Zeigt Detailinformation über das Principal an.

passwd ⟨***principal***⟩ Ändert das Passwort eines Principals.

Hilfe ist zu jeder Zeit durch Eingabe von ⑦ und Enter erhältlich, auch an Prompts, die von Befehlen wie `modify` und `add` ausgegeben werden.

Der Befehl `init`, der benutzt wird, wenn der Realm erstmals erstellt wird (sowie bei einigen anderen), ist im Remote-Modus nicht verfügbar. Um einen neuen Realm zu erstellen, gehen Sie an die Konsole des KDCs und benutzen kadmin im lokalen Modus (mit der Befehlszeilenoption `-l`).

26.6.8 Erstellung von Kerberos Host Principals

Jede Maschine innerhalb Ihres Netzwerks muss einem Kerberos Realm zugeordnet sein und ein KDC kontaktieren können. Außerdem müssen Sie für sie auch ein so genanntes „Host Principal“ anlegen.

Bis jetzt wurden nur Benutzer Credentials behandelt. „Kerberisierte“ Dienste müssen sich im Normalfall aber auch gegenüber dem Client-Benutzer authentifizieren. Hierzu werden so genannte „Host Principals“ für alle Hosts innerhalb eines Realms in der Kerberos Datenbank vorliegen.

Die entsprechende Namenskonvention lautet:
`host/<hostname>@<REALM>`, `hostname` ist hier der vollständige gültige Name des betreffenden Hosts.

Host Principals ähneln in vielerlei Hinsicht normalen Benutzer Principals. Allerdings gibt einige kleine Unterschiede. Der Hauptunterschied zwischen Benutzer Principal und Host Principal liegt darin, dass der Schlüssel des ersteren passwortgeschützt ist. Erhält ein Benutzer ein Ticket-Granting Ticket vom KDC, muss er sein Passwort eingeben, damit Kerberos das Ticket entschlüsseln kann. Für einen Systemadministrator wäre es folglich sehr unbequem, müsste er für den SSH Daemon alle acht Stunden neue Tickets anfordern.

Im Fall der Host Principals wird dieses Problem folgendermaßen gelöst: Der zur Entschlüsselung des ursprünglichen Tickets für den Host Principal erforderliche Schlüssel wird einmal vom Administrator vom KDC angefordert. Anschließend wird dieser Schlüssel in einer lokalen Datei namens `keytab` gespeichert. Dienste wie der SSH Daemon lesen diesen Schlüssel aus und verwenden ihn, um bei Bedarf automatisch neue Schlüssel zu erhalten. Die Standard `keytab` Datei liegt unter `/etc/krb5.keytab`.

Um einen Host Principal für `machine.sample.com` anzulegen, geben Sie während Ihrer kadmin Sitzung Folgendes ein:

```
kinit newbie/admin

newbie/admin@SAMPLE.COM's Password: <type password>

kadmin add -r host/machine.sample.com
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
```

Statt ein Passwort für das neue Principal zu setzen, weist die Option `-r` kadmin an, einen zufälligen Schlüssel zu generieren. Dies ist hier möglich, da wir für diesen Principal keine Benutzeraktivität wünschen. Es ist ein reiner Serveraccount für diese Maschine.

Abschließend extrahieren Sie den Schlüssel und speichern ihn in der lokalen Keytab-Datei `/etc/krb5.keytab`. Diese Datei gehört dem Superuser, weshalb Sie Root sein müssen, um den folgenden Befehl ausführen zu können:

```
ktutil get host/machine.sample.com
```

Danach sorgen Sie bitte dafür, dass Sie das Admin-Ticket mit `kdestroy` vernichten, das Sie via kinit erhalten haben, wie oben beschrieben.

26.6.9 Aktivierung der PAM-Unterstützung für Kerberos

SUSE LINUX wird mit einem PAM-Modul namens `pam_krb5` ausgeliefert, welches die Anmeldung via Kerberos und die Passwortaktualisierung unterstützt. Dieses Modul kann von Anwendungen wie dem Konsole-Login, su und grafischen Anwendungen wie KDM gebraucht werden, in denen der Benutzer ein Passwort eingibt und den Authentifizierungsmechanismus benutzen möchte, um ein erstes Kerberos-Ticket zu erhalten.

Ab dieser Version von SUSE LINUX unterstützt das `pam_unix`-Modul Kerberos-Authentifizierung und Passwortänderungen. Um die Kerberos-Unterstützung in `pam_unix` zu aktivieren, ändern Sie die Datei `/etc/security/pam_unix2.conf` wie folgt:

```
auth:       use_krb5 nullok
account:    use_krb5
password:   use_krb5 nullok
session:    none
```

Wenn diese Datei ausgewertet wird, verwenden alle Dienste Kerberos zur Benutzerauthentifizierung. Falls ein Benutzer keinen Kerberos-Principal besitzt, wird `pam_unix` auf den normalen Password-Authentifizierungsmechanismus zurückgreifen. Das Kerberos-Passwort sollte nun auch transparent mit dem `passwd` Kommando aktualisierbar sein.

Feineinstellungen von `pam_krb5` nehmen Sie über Änderungen der Datei `/etc/krb5.conf` vor und indem Sie Standardapplikationen für `pam` hinzufügen. Details zur Vorgehensweise entnehmen Sie bitte der Manualpage (`man 5 pam_krb5`).

Das Modul `pam_krb5` war ursprünglich **nicht** für Netzwerkdienste bestimmt, die Kerberos-Tickets als Teil der Benutzerauthentifizierung annehmen — dies ist eine ganz andere Geschichte und wird in den folgenden Abschnitten behandelt.

26.6.10 SSH mit Kerberos-Authentifizierung

OpenSSH unterstützt Kerberos-Authentifizierung sowohl in der Protokollversion 1 und 2. Version 1 verwendet eine bestimmte Art von Protokollmeldungen zur Übermittlung von Kerberos Tickets. Version 2 verwendet

Kerberos nicht mehr direkt, sondern greift auf „GSSAPI“, die so genannte *General Security Services API*, zurück. Diese Programmierschnittstelle ist nicht Kerberos spezifisch. Sie wurde entwickelt, um die Eigenheiten des zugrunde liegenden Authentifizierungssystems vor der Anwendung zu verbergen, egal ob dies Kerberos, SPKM oder ein anderes derartiges System ist. Allerdings unterstützt die aktuelle GSSAPI Bibliothek von SUSE LINUX zur Zeit nur Kerberos.

Um sshd mit der Kerberos-Authentifizierung zu benutzen, editieren Sie `/etc/ssh/sshd_config` und setzen die folgenden Optionen:

```
# These are for protocol version 1
KerberosAuthentication yes
KerberosTicketCleanup yes
# These are for version 2 GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

Im Anschluss daran benutzen Sie den Befehl `rcsshd restart`, um Ihren SSH-Daemon neu zu starten.

Wollen Sie Kerberos Authentifizierung mit der Protokollversion 2 nutzen, müssen Sie auch auf der Clientseite die Unterstützung hierfür aktivieren. Entweder Sie erledigen dies systemweit über die Konfigurationsdatei `/etc/ssh/ssh_config` oder auf Benutzerbasis über `~/.ssh/config`. In beiden Fällen müssen Sie der Konfigurationsdatei die Option `GSSAPIAuthentication yes` hinzufügen.

Nun sollten Sie in der Lage sein, eine Verbindung mit Kerberos-Authentifizierung aufzubauen. Verwenden Sie `klist`, um zu überprüfen, ob Sie ein gültiges Ticket für die Verbindungsaufnahme mit dem SSH-Server besitzen. Um die Verwendung des SSH-Protokolls Version 1 zu erzwingen, übergeben Sie die Option `-1` auf der Kommandozeile.

```
ssh earth.sample.com

Last login: Fri Aug  9 14:12:50 2002 from zamboni.sample.com
Have a lot of fun...
```

Hinweis

Weitere Informationen

Lesen Sie in der Datei `/usr/share/doc/packages/openssh/README.kerberos` nach, wie das Zusammenspiel von OpenSSH und Kerberos im Detail geregelt wird.

Hinweis

26.6.11 Benutzung von LDAP und Kerberos

Bei Benutzung von Kerberos bietet sich mit LDAP ein Weg zur Verteilung von Benutzerinformationen (Benutzer-ID, Gruppen, Homeverzeichnisse etc.) im lokalen Netz. Natürlich erfordert dies die Verwendung eines starken Verschlüsselungsmechanismus, um Package-Spoofing etc. zu vermeiden.

Für die LDAP-Kommunikation lässt sich natürlich auch Kerberos verwenden.

OpenLDAP implementiert die meisten der verschiedenen Authentifizierungstypen über SASL, das *Simple Authentication Session Layer*. SASL ist im Grunde ein Netzwerkprotokoll zur Authentifizierung. SUSE LINUX verwendet die cyrus-sasl Implementierung und unterstützt mehrere Authentifizierungstypen. Kerberos Authentifizierung wird über GSSAPI (General Security Services API) umgesetzt.

Standardmäßig ist das SASL-Plugin für GSSAPI nicht installiert. Installieren Sie es von Hand nach:

```
rpm -ivh cyrus-sasl-gssapi-*.rpm
```

Um Kerberos Binding zum OpenLDAP-Server zu ermöglichen, legen Sie einen Principal `ldap/earth.sample.com` an und fügen Sie ihn der `keytab` hinzu:

```
kadmin add -r ldap/earth.sample.com
ktutil get ldap/earth.sample.com
```

An dieser Stelle sollten Sie sich über folgenden Stolperstein klar werden: Der LDAP-Server (slapd) läuft standardmäßig unter Benutzer und Gruppe `ldap`, während `keytab` nur vom Benutzer `root` gelesen werden kann. Also müssen Sie entweder die LDAP-Konfiguration dahingehend abändern, dass der Server als Benutzer `root` gestartet wird oder die `keytab` für die Gruppe `ldap` lesbar machen.

Um slapd als `root` zu betreiben, editieren Sie die Datei `/etc/sysconfig/openldap` und deaktivieren die beiden Variablen `OPENLDAP_USER` and `OPENLDAP_GROUP` durch Einfügen eines Kommentarzeichens am Beginn der Zeile.

Um eine `keytab` Datei für die Gruppe `ldap` lesbar zu machen, gehen Sie folgendermaßen vor:

```
chgrp ldap /etc/krb5.keytab
chmod 640 /etc/krb5.keytab
```

Keine dieser beiden Lösungen ist perfekt. Allerdings ist es momentan nicht möglich, OpenLDAP so zu konfigurieren, dass es eine eigene `keytab` verwendet.

Abschließend starten Sie den LDAP Server mit dem Befehl `rcldap restart` neu.

Kerberos-Authentifizierung mit LDAP

Nun sollten Sie in der Lage sein, Anwendungen wie ldapsearch automatisch mit Kerberos Authentifizierung auszuführen.

```
ldapsearch -b ou=People,dc=suse,dc=de '(uid=newbie)'

SASL/GSSAPI authentication started SASL SSF: 56
SASL installing layers
[...]

# newbie, People, suse.de
dn:uid=newbie,ou=People,dc=suse,dc=de
uid: newbie
cn: Olaf Kirch
[...]
```

Wie Sie hier sehen, gibt ldapsearch eine Meldung aus, dass es GSSAPI Authentifizierung gestartet hat. Die folgende Meldung ist zugegebenermaßen etwas kryptisch — sie gibt den „Security Strenth Factor“ (SSF) mit 56 an. (Der Wert 56 an dieser Stelle ist etwas willkürlich. Sehr wahrscheinlich wurde er so gewählt, weil er die Anzahl der Bits in einem DES Enkryption-Key angibt.) Was Ihnen diese Zeilen im Grunde sagen ist, dass die GSSAPI Authentifizierung erfolgreich war und dass die LDAP-Verbindung per Verschlüsselung geschützt wird.

Vergessen Sie nicht, dass Kerberos Authentifizierung immer ein wechselseitiger Prozess ist. Das bedeutet, nicht nur Sie haben sich gegenüber dem LDAP-Server authentifiziert — er hat sich im Gegenzug auch bei Ihnen authentifiziert. Sie können sich also sicher sein, dass Sie mit dem LDAP-Server kommunizieren, den Sie vorgesehen hatten und nicht mit irgendeinem vorgetäuschten Service, den ein Angreifer aufgesetzt hat.

Für den Fall, dass mehrere verschiedene SASL Mechanismen verwendet werden können, können Sie ldapsearch durch die Kommandozeilenoption `-Y GSSAPI` zur Verwendung von GSSAPI zwingen.

Kerberos-Authentifizierung und LDAP-Zugangskontrollen

Im vorigen Abschnitt haben wir uns erfolgreich am LDAP-Server authentifiziert. Im nächsten Schritt solle es jedem Benutzer ermöglicht werden, das Login-Shell Attribut in seinen LDAP Benutzerdaten zu ändern.

Angenommen, Sie verwenden ein Schema, nach dem der LDAP-Eintrag des Benutzers `joe` unter `uid=joe,ou=people,dc=suse,dc=de` liegt, können Sie die folgenden Zugangsregeln in der Datei `/etc/openldap/slapd.conf` aufstellen:

```
# This is required for things to work _at all_
access to dn.base="" by * read
# Let each user change their login shell
access to dn="*,ou=people,dc=suse,dc=de" attrs=loginShell
       by self write
# Every user can read everything
access to *
       by users read
```

Über die zweite Anweisung erlaubt authentifizierten Benutzern schreibenden Zugriff auf das `loginShell` Attribut ihres LDAP Eintrags. Die dritte Anweisung gibt allen authentifizierten Benutzern Lesezugriff auf das gesamte LDAP-Verzeichnis.

Wie findet nun der LDAP-Server heraus, dass `joe@SAMPLE.COM` von Kerberos das Äquivalent zum LDAP DN (engl. *distinguished name*) `uid=joe,ou=people,dc=suse,dc=de` ist? Diese Zuordnung wir manuell über die `saslExpr` Direktive vorgenommen. Im Beispiel fügen Sie der `slapd.conf` folgende Zeilen hinzu:

```
saslRegexp
        uid=(.*),cn=GSSAPI,cn=auth
        uid=$1,ou=people,dc=example,dc=com
```

Um diesen Mechanismus zu verstehen, sollten Sie wissen, dass OpenLDAP einen DN bildet, wenn SASL einen Benutzer authentifiziert. Dieser DN setzt sich aus dem von SASL übergebenen Namen (wie zum Beispiel `joe`) und dem Typ der SASL Authentifizierung (`GSSAPI`) zusammen. In diesem Fall wäre `uid=joe,cn=GSSAPI,cn=auth` das Ergebnis.

Ist ein `saslRegexp` konfiguriert, wird der LDAP-Server den DN aus der SASL-Information mit dem ersten Argument als regulärem Ausdruck überprüfen. Trifft dieser reguläre Ausdruck zu, wird der Name durch das zweite Argument der `saslRegexp` Anweisung ersetzt. Die Platzhalter (`$1`)

werden durch den Teilausdruck ersetzt, der über den `(.*)` Ausdruck ermittelt wurde.

Selbstverständlich sind auch kompliziertere Suchmuster möglich. Sollten Sie eine kompliziertere Verzeichnisstruktur verwenden oder der Benutzername in dem von Ihnen verwendeten Schema nicht Teil des DN sein, können Sie sogar Suchausdrücke verwenden, die den SASL DN dem Benutzer-DN zuordnen.

26.7 Sicherheit ist Vertrauenssache

26.7.1 Grundlagen

Eines der grundlegendsten Leistungsmerkmale eines Linux/Unix-Systems ist, dass mehrere Benutzer (multiuser) mehrere Aufgaben zur gleichen Zeit auf demselben Rechner (multi-tasking) ausführen können. Das Betriebssystem ist darüber hinaus netzwerktransparent, sodass Benutzer oftmals gar nicht wissen, ob sich die Daten oder Applikationen, mit denen sie arbeiten, lokal auf dem Rechner befinden oder über das Netzwerk bezogen werden.

Damit mehrere Benutzer auf einem System arbeiten können, müssen ihre jeweiligen Daten auch voneinander getrennt verwaltet werden können. Hier geht es unter anderem auch um Sicherheit und den Schutz der Privatsphäre. Datensicherheit war auch schon relevant, als Computer noch nicht miteinander vernetzt waren. Bei Verlust oder Defekt der Datenträger (im Allgemeinen Festplatten) mussten wichtige Daten weiterhin verfügbar sein, auch wenn solche Defekte womöglich den vorübergehenden Ausfall einer größeren Infrastruktur zur Folge hatten.

Auch wenn sich dieses Kapitel des SUSE-Handbuchs in der Hauptsache mit der Vertraulichkeit der Daten und dem Schutz der Privatsphäre der Benutzer beschäftigt, sei betont, dass ein umfassendes Sicherheitskonzept als integralen Bestandteil immer ein regelmäßiges, funktionierendes und überprüftes Backup beinhaltet. Ohne dieses Backup der Daten wird es nicht nur im Fall eines Hardware-Defekts schwierig sein, weiterhin auf die Daten zuzugreifen, sondern insbesondere auch dann, wenn nur der Verdacht besteht, dass jemand sich unbefugterweise an den Daten zu schaffen gemacht hat.

26.7.2 Lokale Sicherheit und Netzwerksicherheit

Es gibt verschiedene Möglichkeiten, auf Daten zuzugreifen:

- Persönliche Kommunikation mit jemand, der über die gewünschten Informationen verfügt bzw. Zugang zu bestimmten Daten auf einem Computer hat,
- direkt an der Konsole eines Rechners (physikalischer Zugriff),
- über eine serielle Schnittstelle oder
- über ein Netzwerk.

Alle diese Fälle sollten eine Gemeinsamkeit haben: Sie sollten sich als Benutzer authentifizieren müssen, bevor Sie Zugriff auf die Ressourcen oder Daten bekommen. Ein Webserver mag da anders geartet sein, aber Sie wollen sicherlich nicht, dass der Webserver Ihre persönlichen Daten an Surfer preisgibt.

Der erste Fall der oben genannten ist der menschlichste von allen: Etwa bei einer Bank müssen Sie einem Angestellten beweisen, dass Ihnen der Zugriff auf Ihre Konten gestattet ist, indem Sie mit Ihrer Unterschrift, einer PIN oder mit einem Passwort beweisen, dass Sie derjenige sind, für den Sie sich ausgeben. In manchen Fällen kann es gelingen, durch das Erwähnen von Kenntnissen oder durch geschickte Rhetorik das Vertrauen eines Wissensträgers zu erschleichen, so dass dieser weitere Information preisgibt, womöglich ohne dass das Opfer dies bemerkt. Man nennt dies in Hackerkreisen Social Engineering. Gegen diese Art von Angriff hilft nur Aufklärung und ein bewusster Umgang mit Information und Sprache. Einbrüchen auf Rechnersystemem geht oft eine Art Social-Engineering-Angriff, etwa auf das Empfangspersonal, Dienstleister in der Firma oder auch Familienmitglieder, voraus, der erst viel später bemerkt wird.

Jemand, der (unbefugt) Zugriff auf Daten erlangen will, könnte auch die traditionellste Methode benutzen, denn die Hardware selbst ist ein Angriffspunkt. Der Rechner muss gegen Entnahme, Austausch und Sabotage von Teilen und Gesamteinheit (und dem Backup der Daten!) sicher verstaut sein - dazu kann auch eine eventuell vorhandene Netzwerkleitung oder ein Stromkabel gehören. Außerdem muss der Startvorgang abgesichert sein, denn allgemein bekannte Tastenkombinationen können den Rechner zu speziellen Reaktionen veranlassen. Dagegen hilft das Setzen von BIOS- und Bootloaderpasswörtern.

Serielle Schnittstellen mit seriellen Terminals sind heute zwar immer noch gebräuchlich, werden aber kaum noch an neuen Arbeitsplätzen installiert. Ein serielles Terminal stellt eine besondere Art des Zugriffs dar: Es ist keine Netzwerkschnittstelle, da kein Netzwerkprotokoll zur Kommunikation zwischen den Systemeinheiten verwendet wird. Ein simples Kabel (oder

eine Infrarotschnittstelle) wird als Übertragungsmedium für einfache Zeichen verwendet. Das Kabel selbst ist dabei der einfachste Angriffspunkt: Man muss nur einen alten Drucker daran anschließen und kann die Kommunikation aufzeichnen. Was mit einem Drucker möglich ist, geht selbstverständlich mit beliebigem Aufwand auch anders.

Da das Öffnen einer Datei auf einem Rechner anderen Zugriffsbeschränkungen unterliegt als das Öffnen einer Netzwerkverbindung zu einem Dienst auf einem Rechner, ist es nötig, zwischen lokaler Sicherheit und Netzwerksicherheit zu unterscheiden. Die Trennlinie ist da markiert, wo Daten in Pakete verschnürt werden müssen, um verschickt zu werden und zur Anwendung zu gelangen.

Lokale Sicherheit

Lokale Sicherheit mit den physikalischen Gegebenheiten, in denen der Rechner aufgestellt ist. Wir gehen davon aus, dass Sie Ihren Rechner so aufgebaut haben, dass das Maß an Sicherheit Ihrem Anspruch und Ihren Anforderungen genügt. In Bezug auf Lokale Sicherheit besteht die Aufgabe darin, die einzelnen Benutzer voneinander zu trennen, sodass kein Benutzer die Rechte oder oder die Identität eines anderen Benutzen annehmen kann. Dies gilt im Allgemeinen, im Speziellen sind natürlich besonders `root`-Rechte gemeint, da der Benutzer `root` im System Allmacht hat; er kann unter anderem ohne Passwort zu jedem lokalen Benutzer werden und jede lokale Datei lesen.

Passwörter

Ihr Linux-System speichert Passwörter nicht etwa im Klartext ab und vergleicht ein eingegebenes Passwort mit dem, was gespeichert ist. Bei einem Diebstahl der Datei, in der die Passwörter stehen, wären dann ja alle Accounts auf Ihrem System kompromittiert. Stattdessen wird Ihr Passwort verschlüsselt abgelegt und jedes Mal, wenn Sie das Passwort eingegeben haben, wird dieses wieder verschlüsselt und das Ergebnis verglichen mit dem, was als verschlüsseltes Passwort abgespeichert ist. Dies macht natürlich nur dann Sinn, wenn man aus dem verschlüsselten Passwort nicht das Klartextpasswort errechnen kann. Dies erreicht man durch so genannte Falltüralgorithmen, die nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann nicht einfach zurückrechnen und das Passwort sehen, sondern er muss alle möglichen Buchstabenkombinationen für ein Passwort durchprobieren, bis er dasjenige findet, welches verschlüsselt so aussieht wie Ihres. Bei acht Buchstaben pro Passwort gibt es beträchtlich viele Kombinationen.

Mit ein Argument für die Sicherheit dieser Methode in den 70er Jahren war, dass der verwendete Algorithmus recht langsam ist und Zeit im Sekundenbereich für das verschlüsseln von einem Passwort brauchte. Heutige PCs schaffen ohne weiteres mehrere hunderttausend bis Millionen Verschlüsselungen pro Sekunde. Aus diesem Grund dürfen verschlüsselte Passwörter nicht für jeden Benutzer sichtbar sein (`/etc/shadow` ist für einen normalen Benutzer nicht lesbar), und die Passwörter dürfen nicht leicht zu erraten sein, für den Fall, dass die verschlüsselten Passwörter wegen eines Fehlers eben doch sichtbar werden. Ein Passwort wie Phantasie umzuschreiben in Ph@nt@s13 hilft nicht viel: Solche Vertauschungsregeln können von Knackprogrammen, die Wörterbücher zum Raten benutzen, sehr leicht aufgelöst werden. Besser sind Kombinationen von Buchstaben, die kein bekanntes Wort bilden und nur für den Benutzer eine persönliche Bedeutung haben, etwa die Anfangsbuchstaben der Wörter eines Satzes, oder nehmen Sie zum Beispiel einen Buchtitel wie Der Name der Rose von Umberto Eco. Daraus gewinnen Sie ein gutes Passwort: DNdRvUE9. Ein Passwort wie Bierjunge oder Jasmin76 würde schon jemand erraten können, der Sie oberflächlich gut kennt.

Der Bootvorgang

Verhindern Sie, dass mit einer Diskette oder einer CD-ROM gebootet werden kann, indem Sie die Laufwerke ausbauen oder indem Sie ein BIOS-Passwort setzen und im BIOS ausschließlich das Booten von Festplatte erlauben.

Linux Systeme starten gewöhnlicherweise mit einem Bootloader, der es erlaubt, zusätzliche Optionen an den zu startenden Kernel weiterzugeben. Solche Optionen sind im hohem Maße sicherheitskritisch, weil der Kernel ja nicht nur mit `root`-Rechten läuft, sondern die `root`-Rechte von Anfang an vergibt. Wenn Sie LILO als Bootloader verwenden, können Sie dies durch Vergabe eines weiteren Passwortes in `/boot/grub/menu.lst` verhindern (siehe 8 auf Seite 223).

Zugriffsrechte

Es gilt das Prinzip, immer mit den niedrigst möglichen Privilegien für eine jeweilige Aufgabe zu arbeiten. Es ist definitiv nicht nötig, seine E-Mails als root zu lesen und zu schreiben. Wenn das Mailprogramm (MUA = Mail User Agent), mit dem Sie arbeiten, einen Fehler hat, dann wirkt sich dieser Fehler mit genau den Rechten aus, die Sie zum Zeitpunkt des des Angriffs hatten. Hier geht es also auch um Schadensminimierung.

Die einzelnen Rechte der weit über 200.000 Dateien einer SUSE-Distribution sind sorgfältig vergeben. Der Administrator eines Systems sollte zusätzliche Software oder andere Dateien nur unter größtmöglicher Sorgfalt installieren und besonders gut auf die vergebenen Rechte der Dateien achten. Erfahrene und sicherheitsbewusste Admins verwenden bei dem Kommando `ls` stets die Option `-l` für eine ausführliche Liste der Dateien mitsamt den Zugriffsrechten, so dass sie eventuell falsch gesetzte Dateirechte gleich erkennen können. Ein falsch gesetztes Attribut bedeutet nicht nur, dass Dateien überschrieben oder gelöscht werden können, sondern auch dass die veränderten Dateien von `root` ausgeführt oder im Fall von Konfigurationsdateien von Programmen als `root` benutzt werden können. Damit könnte ein Angreifer seine Rechte beträchtlich ausweiten. Man nennt solche Angriffe dann Kuckuckseier, weil das Programm (das Ei) von einem fremden Benutzer (Vogel) ausgeführt (ausgebrütet) wird, ähnlich wie der Kuckuck seine Eier von fremden Vögeln ausbrüten lässt.

SUSE-Systeme verfügen über die Dateien `permissions`, `permissions.easy`, `permissions.secure` und `permissions.paranoid` im Verzeichnis `/etc`. In diesen Dateien werden besondere Rechte wie etwa weltschreibbare Verzeichnisse oder für Dateien setuser-ID-bits festgelegt. (Programme mit gesetztem setuser-ID-bit laufen nicht mit der Berechtigung des Eigentümers des Prozesses, der es gestartet hat, sondern mit der Berechtigung des Eigentümers der Datei. Dies ist in der Regel `root`.) Für den Administrator steht die Datei `/etc/permissions.local` zur Verfügung, in der er seine eigenen Änderungen festhalten kann.

Die Auswahl, welche der Dateien für Konfigurationsprogramme von SUSE zur Vergabe der Rechte benutzt werden sollen, können Sie auch komfortabel mit YaST unter dem Menüpunkt 'Sicherheit' treffen. Mehr zu diesem Thema erfahren Sie direkt aus der Datei `/etc/permissions` und der Manpage des Kommandos `chmod` (`man chmod`).

Buffer overflows, format string bugs

Wann immer ein Programm Daten verarbeitet, die in beliebiger Form unter Einfluss eines Benutzers stehen oder standen, ist besondere Vorsicht geboten. Diese Vorsicht gilt in der Hauptsache für den Programmierer der Anwendung: Er muss sicherstellen, dass die Daten durch das Programm richtig interpretiert werden, dass die Daten zu keinem Zeitpunkt in Speicherbereiche geschrieben werden, die eigentlich zu klein sind und dass er die Daten in konsistenter Art und Weise durch sein eigenes Programm und die dafür definierten Schnittstellen weiterreicht.

Ein Buffer Overflow passiert dann, wenn beim Beschreiben eines Pufferspeicherbereichs nicht darauf geachtet wird, wie groß der Puffer eigentlich

ist. Es könnte sein, dass die Daten (die vom Benutzer kamen) etwas mehr Platz verlangen, als im Puffer zur Verfügung steht. Durch dieses Überschreiben des Puffers über seine Grenze hinaus ist es unter Umständen möglich, dass ein Programm aufgrund der Daten, die er eigentlich nur verarbeiten soll, Programmsequenzen ausführt, die unter dem Einfluss des Users und nicht des Programmierers stehen. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Rechten abläuft (siehe Abschnitt 26.7.2 auf Seite 751). Format String Bugs funktionieren etwas anders, verwenden aber wieder user-input, um das Programm von seinem eigentlichen Weg abzubringen.

Diese Programmierfehler werden normalerweise bei Programmen ausgebeutet, die mit gehobenen Privilegien

ausgeführt werden, also setuid- und setgid-Programme. Sie können sich und Ihr System also vor solchen Fehlern schützen, indem Sie die besonderen Ausführungsrechte von den Programmen entfernen. Auch hier gilt wieder das Prinzip der geringstmöglichen Privilegien (siehe Abschnitt 26.7.2 auf Seite 751).

Da Buffer Overflows und Format String Bugs Fehler bei der Behandlung von Benutzerdaten sind, sind sie nicht notwendigerweise nur ausbeutbar, wenn man bereits Zugriff auf ein lokales login hat. Viele der bekannt gewordenen Fehler können über eine Netzwerkverbindung ausgenutzt werden. Deswegen sind Buffer Overflows und Format String Bugs nicht direkt auf den lokalen Rechner oder das Netzwerk klassifizierbar.

Viren

Entgegen andersartiger Verlautbarungen gibt es tatsächlich Viren für Linux. Die bekannten Viren sind von ihren Autoren als Proof-of-Concept geschrieben worden, als Beweis, dass die Technik funktioniert. Allerdings ist noch keiner dieser Viren in freier Wildbahn beobachtet worden.

Viren benötigen zur Ausbreitung einen Wirt, ohne den sie nicht überlebensfähig sind. Dieser Wirt ist ein Programm oder ein wichtiger Speicherbereich für das System, etwa der Master-Boot-Record, und er muss für den Programmcode des Virus beschreibbar sein. Linux hat aufgrund seiner Multi-User Fähigkeiten die Möglichkeit, den Schreibzugriff auf Dateien einzuschränken, also insbesondere Systemdateien. Wenn Sie als `root` arbeiten, erhöhen Sie also die Wahrscheinlichkeit, dass Ihr System von solch einem Virus infiziert wird. Berücksichtigen Sie aber die Regel der geringstmöglichen Privilegien, ist es Schwierigkeiten unter Linux einen Virus zu bekommen. Darüber hinaus sollten Sie nie leichtfertig ein Programm ausführen, das Sie aus dem Internet bezogen haben und dessen genaue Herkunft Sie nicht kennen. SUSE-rpm Pakete sind kryptographisch signiert

und tragen mit dieser digitalen Unterschrift das Markenzeichen der Sorgfalt beim Bau der Pakete bei SUSE. Viren sind klassische Symptome dafür, dass auch ein hochsicheres System unsicher wird, wenn der Administrator oder auch der Benutzer ein mangelndes Sicherheitsbewusstsein hat.

Viren sind nicht mit Würmern zu verwechseln, die Phänomene auch der Netzwerksicherheit sind und keinen Wirt brauchen, um sich zu verbreiten.

Netzwerksicherheit

Bei der lokalen Sicherheit war es die Aufgabe, die Benutzer, die an demselben Rechner arbeiten, voneinander zu trennen, insbesondere den Benutzer `root`. Im Gegensatz dazu soll bei der Netzwerksicherheit das ganze System gegen Angriffe über das Netzwerk geschützt werden. Benutzerauthentifizierung beim klassischen Einloggen durch Benutzerkennung und Passwort gehört zur lokalen Sicherheit. Beim Einloggen über eine Netzwerkverbindung muss man differenzieren zwischen beiden Sicherheitsaspekten: bis zur erfolgten Authentifizierung spricht man von Netzwerksicherheit, nach dem Login geht es um lokale Sicherheit.

X-Windows (X11-Authentifizierung)

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X11, dem Windowing-System von Unix, gilt dies in besonderem Maße! Sie können sich ohne Weiteres auf einem entfernten Rechner einloggen und dort ein Programm starten, welches dann über das Netzwerk auf Ihrem Rechner angezeigt wird.

Wenn nun ein X-Client über das Netzwerk bei unserem X-Server angezeigt werden soll, dann muss der Server die Ressource, die er verwaltet (das Display), gegen unberechtigte Zugriffe schützen. Konkret heißt das hier, dass das Client-Programm Rechte bekommen muss. Bei X-Windows geschieht dies auf zwei verschiedene Arten: Host-basierte und cookie-basierte Zugriffskontrolle. Erstere basiert auf der IP-Adresse des Rechners, auf dem das Client-Programm laufen soll und wird mit dem Programm `xhost` kontrolliert. Das Programm `xhost` trägt eine IP-Adresse eines legitimen Client in eine Mini-Datenbank im X-Server ein. Eine Authentifizierung einzig und allein auf einer IP-Adresse aufzubauen gilt jedoch nicht gerade als sicher. Es könnte noch ein zweiter Benutzer auf dem Rechner mit dem Client-Programm aktiv sein, und dieser hätte dann genau wie jemand, der die IP-Adresse stiehlt, Zugriff auf den X-Server. Deswegen soll hier auch nicht näher auf diese Methoden eingegangen werden. Die Manpage des `xhost`-Kommandos gibt mehr Aufschluss über die Funktionsweise (und enthält ebenfalls die Warnung!).

Bei cookie-basierter Zugriffskontrolle wird eine Zeichenkette, die nur der X-Server und der legitim eingeloggte Benutzer kennen, als einem Passwort ähnliches Ausweismittel verwendet. Dieses cookie (das englische Wort cookie bedeutet Keks und meint hier die chinesischen fortune cookies, die einen Spruch enthalten) wird in der Datei `.Xauthority` im home-Verzeichnis des Benutzers beim login abgespeichert und steht somit jedem X-Windows-client, der ein Fenster beim X-Server zur Anzeige bringen will, zur Verfügung. Das Programm `xauth` gibt dem Benutzer das Werkzeug, die Datei `.Xauthority` zu untersuchen. Wenn Sie `.Xauthority` aus Ihrem home-Verzeichnis löschen oder umbenennen, dann können Sie keine weiteren Fenster von neuen X-Clients mehr öffnen. Näheres über Sicherheitsaspekte von X-Windows erfahren Sie in der manpage von `Xsecurity` (`man Xsecurity`).

`ssh` (secure shell) kann über eine vollständig verschlüsselte Netzverbindung für einen Benutzer transparent (also nicht direkt sichtbar) die Verbindung zu einem X-Server weiterleiten. Man spricht von X11-forwarding. Dabei wird auf der Server-Seite ein X-Server simuliert und bei der Shell auf der remote-Seite die DISPLAY-Variable gesetzt.

Achtung

Wenn Sie den Rechner, auf dem Sie sich einloggen, nicht als sicher betrachten, dann sollten Sie auch keine X-Windows-Verbindungen weiterleiten lassen. Mit eingeschaltetem X11-forwarding könnten sich auch Angreifer über Ihre ssh-Verbindung mit Ihrem X-Server authentifiziert verbinden und beispielsweise Ihre Tastatur belauschen.

Achtung

Buffer Overflows und Format String Bugs

Nicht direkt klassifizierbar in lokal und remote gilt das im Abschnitt Lokale Sicherheit über Buffer Overflows und Format String Bugs Gesagte äquivalent für Netzwerksicherheit. Wie auch bei den lokalen Varianten dieser Programmierfehler führen Buffer Overflows bei Netzwerkdiensten meistens zu `root`-Rechten. Sollte dies nicht der Fall sein, dann könnte sich der Angreifer zumindest Zugang zu einem unpriviligierten lokalen Account verschaffen, mit dem er dann weitere (lokale) Sicherheitsprobleme ausnutzen kann, falls diese vorhanden sind.

Über das Netzwerk ausbeutbare Buffer Overflows und Format String Bugs sind wohl die häufigsten Varianten von remote-Angriffen überhaupt. Auf

Sicherheitsmailinglisten werden so genannte *exploits* herumgereicht, d. h. Programme, die die frisch gefundenen Lücken ausnutzen. Auch jemand, der nicht die genauen Details der Lücke kennt, kann damit die Lücke ausnutzen. Im Laufe der Jahre hat sich herausgestellt, dass die freie Verfügbarkeit von exploitcodes generell die Sicherheit von Betriebssystemen erhöht hat, was sicherlich daran liegt, dass Betriebssystemhersteller dazu gezwungen waren, die Probleme in ihrer Software zu beseitigen. Da bei freier Software der Sourcecode für jedermann erhältlich ist (SUSE-Linux liefert alle verfügbaren Quellen mit), kann jemand, der eine Lücke mitsamt exploitcode findet, auch gleichzeitig noch einen Reparaturvorschlag für das Problem anbieten.

DoS — Denial of Service

Ziel dieser Art von Angriff ist das Blockieren eines Dienstes oder sogar des ganzen Systems. Dies kann auf verschiedenste Arten passieren: Durch Überlastung, durch Beschäftigung mit unsinnigen Paketen oder durch Ausnutzen von Remote Buffer Overflows, die nicht direkt zum Ausführen von Programmen auf der remote-Seite ausbeutbar sind.

Der Zweck eines DoS mag meistens darin begründet sein, dass der Dienst einfach nicht mehr verfügbar ist. Dass ein Dienst fehlt, kann aber weitere Konsequenzen haben. Siehe man in the middle: sniffing, tcp connection hijacking, spoofing und DNS poisoning.

man in the middle: sniffing, tcp connection hijacking, spoofing

Ganz allgemein gilt: Ein Angriff vom Netzwerk, bei der der Angreifer eine Position zwischen zwei Kommunikationspartnern einnimmt, nennt sich man in the middle attack. Sie haben in der Regel eines gemeinsam: Das Opfer merkt nichts davon. Viele Varianten sind denkbar: Der Angreifer nimmt die Verbindung entgegen und stellt, damit das Opfer nichts merkt, selbst eine Verbindung zum Ziel her. Das Opfer hat also, ohne es zu wissen, eine Netzwerkverbindung zum falschen Rechner geöffnet, weil dieser sich als das Ziel ausgibt. Der einfachste man in the middle attack ist ein sniffer. Er belauscht einfach nur die Netzverbindungen, die an ihm vorüber geführt werden (sniffing = engl. schnüffeln). Komplexer wird es, wenn der Angreifer in der Mitte versucht, eine etablierte, bestehende Verbindung zu übernehmen (entführen = engl. hijacking). Dafür muss der Angreifer die Pakete, die an ihm vorbeigeführt werden, eine Weile lang analysiert haben, damit er die richtigen TCP-Sequenznummern der TCP-Verbindung vorhersagen kann. Wenn er dann die Rolle des Ziels der Verbindung übernimmt, merkt

das das Opfer, weil auf der Seite des Opfers die Verbindung als ungültig terminiert wird.

Der Angreifer profitiert dabei insbesondere bei Protokollen, die nicht kryptographisch gegen hijacking gesichert sind und bei denen zu Beginn der Verbindung einen Authentifizierung stattfindet. Spoofing nennt sich das Verschicken von Paketen mit modifizierten Absenderdaten, also hauptsächlich der IP Adresse. Die meisten aktiven Angriffsvarianten verlangen das Verschicken von gefälschten Paketen, was unter Unix/Linux übrigens nur der Superuser (`root`) darf.

Viele der Angriffsmöglichkeiten kommen in Kombination mit einem DoS vor. Gibt es eine Möglichkeit, einen Rechner schlagartig vom Netzwerk zu trennen (wenn auch nur für kurze Zeit), dann wirkt sich das förderlich auf einen aktiven Angriff aus, weil keine Störungen mehr erwartet werden müssen.

DNS poisoning

Der Angreifer versucht, mit gefälschten („gespooften") DNS-Antwortpaketen den cache eines DNS-Servers zu vergiften (engl. *poisoning*), so dass dieser die gewünschte Information an ein Opfer weitergibt, das danach fragt. Um einem DNS-Server solche falschen Informationen glaubhaft zuschieben zu können, muss der Angreifer normalerweise einige Pakete des Servers bekommen und analysieren. Weil viele Server ein Vertrauensverhältnis zu anderen Rechnern aufgrund ihrer IP Adresse oder ihres Hostnamens konfiguriert haben, kann ein solcher Angriff trotz eines gehörigen Aufwands recht schnell Früchte tragen. Voraussetzung ist allerdings eine gute Kenntnis der Vertrauensstruktur zwischen diesen Rechnern. Ein zeitlich genau abgestimmter DoS gegen einen DNS-Server, dessen Daten gefälscht werden sollen, ist aus Sicht des Angreifers meistens nicht vermeidbar.

Abhilfe schafft wieder eine kryptographisch verschlüsselte Verbindung, die die Identität des Ziels der Verbindung verifizieren kann.

Würmer

Würmer werden häufig mit Viren gleichgesetzt. Es gibt aber einen markanten Unterschied: Ein Wurm muss keinerlei Wirtsprogramm infizieren, und er ist darauf spezialisiert, sich möglichst schnell im Netzwerk zu verbreiten. Bekannte Würmer wie Ramen, Lion oder Adore nutzen wohlbekannte Sicherheitslücken von Serverprogrammen wie `bind8` oder `lprNG`. Man kann sich relativ einfach gegen Würmer schützen, weil zwischen dem Zeitpunkt des Bekanntwerdens der ausgenutzten Lücken bis zum Auftauchen

des Wurms normalerweise einige Tage vergehen, so dass update-Pakete vorhanden sind. Natürlich setzt dies voraus, dass der Administrator die Security-updates auch in seine Systeme einspielt.

26.7.3 Tipps und Tricks: Allgemeine Hinweise

Information: Für einen effizienten Umgang mit dem Bereich Sicherheit ist es nötig, mit den Entwicklungen Schritt zu halten und auf dem Laufenden zu sein, was die neuesten Sicherheitsprobleme angeht. Ein sehr guter Schutz gegen Fehler aller Art ist das schnellstmögliche Einspielen von update-Paketen, die von einem Security-Announcement angekündigt werden. Die SUSE-security-Announcements werden über eine Mailingliste verbreitet, in die Sie sich, den Links unter `http://www.suse.de/security` folgend, eintragen können. `suse-security-announce@suse.de` ist die erste Informationsquelle für update-Pakete, die vom Security-Team mit neuen Informationen beliefert wird.

Die Mailingliste `suse-security@suse.de` ist ein lehrreiches Diskussionsforum für den Bereich Sicherheit. Sie können sich auf der gleichen URL wie für `suse-security-announce@suse.de` für die Liste anmelden.

Eine der bekanntesten Sicherheitsmailinglisten der Welt ist die Liste `bugtraq@securityfocus.com`. Die Lektüre dieser Liste bei durchschnittlich 15-20 Postings am Tag kann mit gutem Gewissen empfohlen werden. Mehr Information finden Sie auf `http://www.securityfocus.com`.

Einige Grundregeln, die zu kennen nützlich sein kann, sind nachstehend aufgeführt:

- Vermeiden Sie es, als `root` zu arbeiten, entsprechend dem Prinzip, die geringstnötigen Privilegien für eine Aufgabe zu benutzen. Das verringert die Chancen für ein Kuckucksei oder einen Virus, und überdies für Fehler Ihrerseits.
- Benutzen Sie nach Möglichkeit immer verschlüsselte Verbindungen, um Arbeiten remote auszuführen. `ssh` (secure shell) ist Standard, vermeiden Sie `telnet`, `ftp`, `rsh` und `rlogin`.
- Benutzen Sie keine Authentifizierungsmethoden, die alleine auf der IP-Adresse aufgebaut sind.
- Halten Sie Ihre wichtigsten Pakete für den Netzwerkbereich immer auf dem neuesten Stand und abonnieren Sie die Mailinglisten

für Announcements der jeweiligen Software (z. B. Beispiel `bind`, `sendmail`, `ssh`). Dasselbe gilt für Software, die nur lokale Sicherheitsrelevanz hat.

- Optimieren Sie die Zugriffsrechte auf sicherheitskritische Dateien im System, indem Sie die `/etc/permissions`-Datei Ihrer Wahl an Ihre Bedürfnisse anpassen. Ein setuid-Programm, welches kein setuid-bit mehr hat, mag zwar nicht mehr wirklich seine Aufgabe erledigen können, aber es ist in der Regel kein Sicherheitsproblem mehr. Mit einer ähnlichen Vorgehensweise können Sie auf welt-schreibbare Dateien und Verzeichnisse losgehen.

- Deaktivieren Sie jegliche Netzwerkdienste, die Sie auf Ihrem Server nicht zwingend brauchen. Das macht Ihr System sicherer, und es verhindert, dass Ihre Benutzer sich an einen Dienst gewöhnen, den Sie nie absichtlich freigegeben haben (legacy-Problem). Offene Ports (mit socket-Zustand LISTEN) finden Sie mit dem Programm `netstat`. Als Optionen bietet sich an, `netstat -ap` oder `netstat -anp` zu verwenden. Mit der `-p`-Option können Sie gleich sehen, welcher Prozess mit welchem Namen den Port belegt.

  Vergleichen Sie die Ergebnisse, die Sie haben, mit einem vollständigen Portscan Ihres Rechners von außen. Das Programm `nmap` ist dafür hervorragend geeignet. Es klopft jeden einzelnen Port ab und kann anhand der Antwort Ihres Rechners Schlüsse über einen hinter dem Port wartenden Dienst ziehen. Scannen Sie niemals einen Rechner ohne das direkte Einverständnis des Administrators, denn dies könnte als aggressiver Akt aufgefasst werden. Denken Sie daran, dass Sie nicht nur TCP-Ports scannen sollten, sondern auf jeden Fall auch UDP-Ports (Optionen `-sS` und `-sU`).

- Zur zuverlässigen Integritätsprüfung der Dateien in Ihrem System sollten Sie `tripwire` benutzen und die Datenbank verschlüsseln, um sie gegen manipulative Zugriffe zu schützen. Darüber hinaus brauchen Sie auf jeden Fall ein Backup dieser Datenbank außerhalb der Maschine auf einem eigenen Datenträger, der nicht über einen Rechner mit einem Netzwerk verbunden ist.

- Seien Sie vorsichtig beim Installieren von Fremdsoftware. Es gab schon Fälle, wo ein Angreifer tar-Archive einer Sicherheitssoftware mit einem trojanischen Pferd versehen hat. Zum Glück wurde dies schnell bemerkt. Wenn Sie ein binäres Paket installieren, sollten Sie sicher sein, woher das Paket kommt.

SUSE rpm-Pakete werden gpg-signiert ausgeliefert. Der Schlüssel, den wir zum Signieren verwenden, ist

ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

Das Kommando `rpm -checksig paket.rpm` zeigt an, ob die Prüfsumme und die Signatur des (nicht installierten!) Pakets stimmen. Sie finden den Schlüssel auf der ersten CD oder DVD von SUSE LINUX und auf den meisten Keyservern der Welt.

- Überprüfen Sie regelmäßig Ihr Backup der Daten und des Systems. Ohne eine zuverlässige Aussage über die Funktion des Backups ist das Backup unter Umständen wertlos.
- Überwachen Sie Ihre Logfiles. Nach Möglichkeit sollten Sie sich ein kleines Script schreiben, welches Ihre Logfiles nach ungewöhnlichen Einträgen absucht. Diese Aufgabe ist alles andere als trivial, denn nur Sie wissen, was ungewöhnlich ist und was nicht.
- Verwenden Sie `tcp_wrapper`, um den Zugriff auf die einzelnen Dienste Ihres Rechners auf die IP-Adressen einzuschränken, denen der Zugriff auf einen bestimmten Dienst explizit gestattet ist. Nähere Information zu den `tcp_wrappern` finden Sie in der Manualpage von `tcpd(8)` und der Manualpage von `hosts_access`.
- Als zusätzlichen Schutz zu dem `tcpd` (tcp_wrapper) könnten Sie die SuSEfirewall verwenden.
- Legen Sie Ihr Sicherheitsdenken redundant aus: Eine Meldung, die zweimal eintrifft, ist besser als eine, die Sie nie sehen. Dies gilt genauso für Gespräche mit Kollegen.

26.7.4 Zentrale Meldung neuer Sicherheitsproblemen

Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie die zur Verfügung stehenden Update-Pakete), dann wenden Sie sich bitte vertrauensvoll an die E-Mail-Adresse `mailto:security@suse.de`. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. Wir werden uns bemühen, Ihnen so schnell wie möglich zu antworten. Eine pgp-Verschlüsselung Ihrer E-Mail ist erwünscht. Unser pgp-Key ist:

ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>

Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5

Der Schlüssel liegt auch unter `http://www.suse.de/security` zum Download bereit.

Teil IV

Administration

Access Control Lists unter Linux

Dieses Kapitel gibt einen kurzen Einblick in die Hintergründe und Funktionsweise von POSIX ACLs für Linux-Dateisysteme. Sie erfahren, wie das traditionelle Rechtekonzept für Dateisystemobjekte mit Hilfe von ACLs (*Access Control Lists*) erweitert wird und welche Vorteile dieses Konzept bietet.

27.1 Warum ACLs? 766
27.2 Definitionen 767
27.3 Umgang mit ACLs 768
27.4 Unterstützung in Anwendungen 777

27.1 Warum ACLs?

Hinweis

POSIX ACLs

Der Ausdruck *POSIX ACL* suggeriert, dass es sich um einen echten Standard aus der POSIX (*Portable Operating System Interface*) Familie handelt. Aus verschiedenen Gründen wurden die betreffenden Standardentwürfe POSIX 1003.1e und POSIX 1003.2c zurückgezogen. ACLs unter vielen UNIX-artigen Betriebssystemen basieren allerdings auf diesen Entwürfen. Die in diesem Kapitel beschriebene Implementierung von Dateisystem ACLs folgt den Inhalten dieser beiden Dokumente, die Sie unter folgender URL einsehen können:
`http://wt.xpilot.org/publications/posix.1e/`

Hinweis

Traditionell sind für jedes Dateiobjekt unter Linux drei Sets von Berechtigungen definiert. Diese Sets geben die Lese- (`r`), Schreib- (`w`) und Ausführungsrechte (`x`) für die drei Benutzerklassen Eigentümer der Datei (engl. *owner*), Gruppe (engl. *group*) und „Rest der Welt“ (engl. *other*) wieder. Zusätzlich können noch die *set user id*, *set group id* und *sticky* Bits gesetzt werden. Mehr zu diesem Thema finden Sie im *Benutzerhandbuch* im Abschnitt *Benutzer und Zugriffsrechte*.

Für die meisten in der Praxis auftretenden Fälle reicht dieses schlanke Konzept völlig aus. Für komplexere Szenarien oder fortgeschrittenere Anwendungen mussten Systemadministratoren zuvor eine Reihe von Tricks anwenden, um die Einschränkungen des traditionellen Rechtekonzepts zu umgehen.

In Situationen, in denen das traditionelle Dateirechte-Konzept nicht ausreicht, helfen ACLs. Sie erlauben es, einzelnen Benutzern oder Gruppen Rechte zuzuweisen, auch wenn diese nicht mit dem Eigentümer oder der Gruppe einer Datei übereinstimmen.

Access Control Lists sind ein Feature des Linux-Kernels und werden zur Zeit von ReiserFS, Ext2, Ext3, JFS und XFS unterstützt. Mit ihrer Hilfe können komplexe Szenarien umgesetzt werden, ohne dass auf Applikationsebene komplexe Rechtemodelle implementiert werden müssten.

Ein prominentes Beispiel für die Vorzüge von Access Control Lists ist der Austausch eines Windows-Servers gegen einen Linux-Server. Manche der

angeschlossenen Workstations werden auch nach dem Umstieg weiter unter Windows betrieben werden. Das Linux-System bietet den Windows-Clients via Samba Datei- und Druckserver-Dienste an.

Da Samba Access Control Lists unterstützt, können Benutzerrechte sowohl auf dem Linux-Server als auch über eine grafische Benutzeroberfläche unter Windows (nur Windows NT und höher) eingerichtet werden. Über den winbindd ist es sogar möglich, Benutzern Rechte einzuräumen, die nur in der Windows-Domain existieren und über keinen Account auf dem Linux-Server verfügen. Auf der Serverseite können Sie die Access Control Lists mithilfe von getfacl und setfacl bearbeiten.

27.2 Definitionen

Benutzerklassen Das herkömmliche POSIX Rechtekonzept kennt drei *Klassen* von Benutzern für die Rechtevergabe im Dateisystem: Eigentümer (engl. *owner*), Gruppe (engl. *group*) und andere Benutzer oder den „Rest der Welt“ (engl. *other*). Pro Benutzerklasse lassen sich jeweils die drei Berechtigungsbits (engl. *permission bits*) für Lesezugriff (`r`), für Schreibzugriff (`w`) und für Ausführbarkeit (`x`) vergeben. Eine Einführung in das Benutzerkonzept unter Linux finden Sie im *Benutzerhandbuch* im Abschnitt *Benutzer und Zugriffsrechte*.

Access ACL Die Zugriffsrechte für Benutzer und Gruppen auf beliebige Dateisystemobjekte (Dateien und Verzeichnisse) werden über Access ACLs (dt. *Zugriffs-ACLs*) festgelegt.

Default ACL Default ACLs (dt. *Vorgabe-ACLs*) können nur auf Verzeichnisse angewandt werden und legen fest, welche Rechte ein Dateisystemobjekt von seinem übergeordneten Verzeichnis beim Anlegen erbt.

ACL-Eintrag Jede ACL besteht aus einem Satz von ACL-Einträgen (engl. *ACL entries*). Ein ACL-Eintrag hat einen Typ (siehe Tabelle 27.1 auf der nächsten Seite), einen Bezeichner für den Benutzer oder die Gruppe, auf die sich dieser Eintrag bezieht, und Berechtigungen. Der Bezeichner für Gruppe oder Benutzer bleibt für einige Typen von Einträgen leer.

27.3 Umgang mit ACLs

Im folgenden Abschnitt lernen Sie den Grundaufbau einer ACL und deren verschiedene Ausprägungen kennen. Der Zusammenhang zwischen ACLs und dem traditionellen Rechtekonzept im Linux-Dateisystem wird anhand mehrerer Grafiken kurz erläutert. An zwei Beispielen lernen Sie, selbst ACLs zu erstellen und deren korrekte Syntax zu beachten. Zuletzt erfahren Sie, nach welchem Muster ACLs vom Betriebssystem ausgewertet werden.

27.3.1 Aufbau von ACL-Einträgen

ACLs werden grundsätzlich in zwei Klassen eingeteilt. Eine *minimale* ACL besteht ausschließlich aus den Einträgen vom Typ *owner* (Besitzer), *owning group* (Besitzergruppe) und *other* (Andere), und entspricht den herkömmlichen Berechtigungsbits für Dateien und Verzeichnisse. Eine *erweiterte* (engl. *extended*) ACL geht über dieses Konzept hinaus. Sie muss einen *mask* (Maske) Eintrag enthalten und darf mehrere Einträge des Typs *named user* (namentlich gekennzeichneter Benutzer) und *named group* (namentlich gekennzeichnete Gruppe) enthalten. Tabelle 27.1 fasst die verschiedenen verfügbaren Typen von ACL-Einträgen zusammen.

Tabelle 27.1: *Überblick: Typen von ACL-Einträgen*

Typ	Textform
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`
named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

In den Einträgen *owner* und *other* festgelegte Rechte sind immer wirksam. Vom *mask* Eintrag abgesehen, können alle übrigen Einträge (*named user*, *owning group* und *named group*) entweder wirksam oder maskiert werden. Sind Rechte sowohl in einem der oben genannten Einträge als auch in der Maske vorhanden, werden sie wirksam. Rechte, die nur in der Maske oder

nur im eigentlichen Eintrag vorhanden sind, sind nicht wirksam. Das nachfolgende Beispiel verdeutlicht diesen Mechanismus (siehe Tabelle 27.2):

Tabelle 27.2: *Maskierung von Zugriffsrechten*

Typ	Textform	Rechte
named user	`user:jane:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	Wirksame Berechtigungen:	`r--`

27.3.2 ACL-Einträge und Berechtigungsbits

Die beiden Abbildungen illustrieren die beiden auftretenden Fälle einer minimalen und einer erweiterten ACL (siehe Abb. 27.1 und 27.2 auf der nächsten Seite). Die Abbildungen gliedern sich in drei Blöcke. Links die Typangaben der ACL-Einträge, in der Mitte eine beispielhafte ACL und rechts die entsprechenden Berechtigungsbits, wie sie auch `ls -l` anzeigt.

In beiden Fällen werden die *owner class* Berechtigungen dem *owner* ACL-Eintrag zugeordnet. Die Zuordnung der *other class* Berechtigungen zum entsprechenden ACL-Eintrag ist ebenfalls konstant. Die Zuordnung der *group class* Berechtigungen variiert:

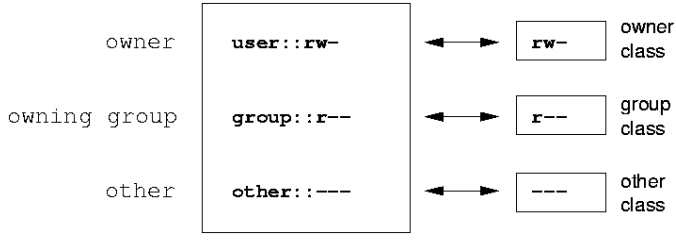

Abbildung 27.1: *Minimale ACL: ACL-Einträge vs. Berechtigungsbits*

- Im Fall einer minimalen ACL — ohne *mask* Eintrag — werden die *group class* Berechtigungen dem *owning group* ACL-Eintrag zugeordnet (siehe Abb. 27.1).

- Im Fall einer erweiterten ACL — mit *mask* Eintrag — werden die *group class* Berechtigungen dem *mask* Eintrag zugeordnet (siehe Abb. 27.2).

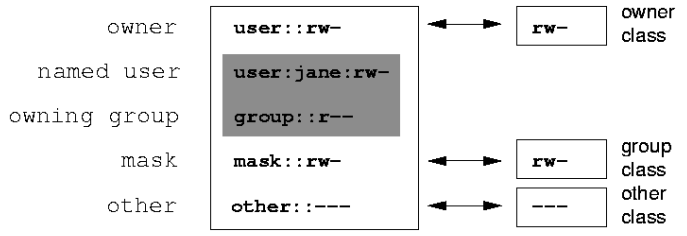

Abbildung 27.2: *Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits*

Durch diese Art der Zuordnung ist die reibungslose Interaktion von Anwendungen mit und ohne ACL-Unterstützung gewährleistet. Die Zugriffsrechte, die mittels der Berechtigungsbits festgelegt wurden, sind die Obergrenze für alle anderen „Feineinstellungen“, die per ACL gemacht werden. Alle Rechte, die hier nicht widergespiegelt sind, wurden entweder in der ACL nicht gesetzt oder sind nicht effektiv. Werden Berechtigungsbits geändert, spiegelt sich dies in der ACL wider und umgekehrt.

27.3.3 Ein Verzeichnis mit Access ACL

In drei Schritten werden Sie anhand folgendem Beispiel den Umgang mit einer Access ACL lernen:

- Anlegen eines Dateisystemobjekts (hier eines Verzeichnisses)
- Änderungen an der ACL
- Einsatz von Masken

1. Bevor Sie das Verzeichnis anlegen, können Sie mittels des `umask` Befehls festlegen, welche Zugriffsrechte gleich bei der Erstellung maskiert werden sollen:

   ```
   umask 027
   ```

`umask 027` beschränkt die Rechte der einzelnen Benutzergruppen folgendermaßen: der Besitzer der Datei behält sämtliche Rechte (`0`), die Besitzergruppe darf nicht schreibend auf die Datei zugreifen (`2`) und alle anderen Benutzer erhalten keinerlei Zugriff (`7`). Die Zahlen sind als Bitmaske zu lesen. Details zu `umask` entnehmen Sie der entsprechenden Manualpage (`man umask`).

```
mkdir mydir
```

Das Verzeichnis `mydir/` ist angelegt und hat die durch die `umask` festgelegten Rechte erhalten. Mit

```
ls -dl mydir
```

```
drwxr-x--- ... tux projekt3 ... mydir
```

überprüfen Sie, ob alle Rechte korrekt vergeben wurden.

2. Nachdem Sie sich über den Ausgangszustand der ACL informiert haben, fügen Sie ihr jeweils einen neuen Benutzer- und Gruppen-Eintrag hinzu.

```
getfacl mydir
```

```
# file: mydir
# owner: tux
# group: projekt3
user::rwx
group::r-x
other::---
```

Die Ausgabe von `getfacl` spiegelt exakt die unter Abschnitt 27.3.2 auf Seite 769 beschriebene Zuordnung von Berechtigungsbits und ACL-Einträgen wider. Die ersten drei Zeilen der Ausgabe nennen Namen, Eigentümer und zugehörige Gruppe des Verzeichnisses. Die drei nächsten Zeilen enthalten die drei ACL-Einträge *owner*, *owning group* und *other*. Insgesamt liefert Ihnen der `getfacl` Befehl im Fall dieser einfachsten („minimalen“) ACL keine Information, die Sie mittels `ls` nicht auch erhalten hätten.

Ihr erster Eingriff in die ACL besteht darin, einem zusätzlichen Benutzer `jane` und einer zusätzlichen Gruppen `djungle` Lese-, Schreib- und Ausführrechte zu gewähren.

```
setfacl -m user:jane:rwx,group:djungle:rwx mydir
```

Die Option `-m` weist `setfacl` an, die bestehende ACL zu modifizieren. Das nachfolgende Argument gibt an, welche ACL-Einträge geändert werden (mehrere werden durch Kommata voneinander getrennt). Abschließend geben Sie den Namen des Verzeichnisses an, für das diese Änderungen gelten sollen.

Die resultierende ACL geben Sie wieder mit `getfacl` aus.

```
# file: mydir
# owner: tux
# group: projekt3
user::rwx
user:jane:rwx
group::r-x
group:djungle:rwx
mask::rwx
other::---
```

Zusätzlich zu den von Ihnen initiierten Einträgen für den Benutzer `jane` und die Gruppe `djungle` wurde ein *mask* Eintrag erzeugt. Dieser *mask* Eintrag wird automatisch gesetzt, um alle Einträge in der *group class* auf einen gemeinsamen Nenner zu bringen. Außerdem passt `setfacl` bestehende *mask* Einträge an von Ihnen geänderte Einstellungen automatisch an, so Sie das nicht mit `-n` deaktivieren. *mask* legt die maximal wirksamen Zugriffsrechte für alle Einträge innerhalb der *group class* fest. Dies beinhaltet: *named user*, *named group* und *owning group*. Die *group class* Berechtigungsbits, die ein `ls -dl mydir` ausgeben würde, entsprechen jetzt dem `mask`-Eintrag.

```
ls -dl mydir

drwxrwx---+ ... tux projekt3 ... mydir
```

Es erscheint in der ersten Spalte der Ausgabe ein `+`, das auf eine *erweiterte* ACL hinweist.

3. Gemäß der Ausgabe des `ls` Kommandos beinhalten die Rechte für den *mask* Eintrag auch Schreibzugriff. Traditionell würden diese Berechtigungsbits auch darauf hinweisen, dass die *owning group* (hier: `projekt3`) ebenfalls Schreibzugriff auf das Verzeichnis `mydir/` hätte. Allerdings sind die wirklich wirksamen Zugriffsrechte für die *owning group* als die Schnittmenge aus den für *owning group* und *mask* gesetzten Rechten definiert; also in unserem Beispiel `r-x` (siehe Tabelle 27.2 auf Seite 769). Es hat sich auch nach Hinzufügen der ACL-Einträge nichts an den Rechten der *owning group* geändert.

Verändern können Sie den *mask* Eintrag mittels `setfacl` oder `chmod`.

```
chmod g-w mydir
ls -dl mydir

drwxr-x---+ ... tux projekt3 ... mydir

getfacl mydir

# file: mydir
# owner: tux
# group: projekt3
user::rwx
user:jane:rwx          # effective: r-x
group::r-x
group:djungle:rwx      # effective: r-x
mask::r-x
other::---
```

Nachdem Sie per `chmod` die *group class* Bits um den Schreibzugriff verringert haben, liefert Ihnen schon die Ausgabe des `ls` Kommandos den Hinweis darauf, dass die *mask* Bits über `chmod` entsprechend angepasst wurden. Man erkennt, dass nur der Besitzer Schreibberechtigung im Verzeichnis `mydir/` hat. Noch deutlicher wird dies an der Ausgabe von `getfacl`. `getfacl` fügt für alle Einträge Kommentare hinzu, deren tatsächlich wirksame Berechtigungsbits nicht mit den ursprünglich gesetzten übereinstimmen, weil sie vom *mask* Eintrag herausgefiltert werden. Sie können den Ausgangszustand mit dem entsprechenden `chmod` Kommando wiederherstellen:

```
chmod g+w mydir
ls -dl mydir

drwxrwx---+ ... tux projekt3 ... mydir

getfacl mydir

# file: mydir
# owner: tux
# group: projekt3
user::rwx
user:jane:rwx
group::r-x
group:djungle:rwx
```

```
mask::rwx
other::---
```

27.3.4 Ein Verzeichnis mit Default ACL

Verzeichnisse können mit einer besonderen Art von ACLs versehen werden; einer Default ACL. Diese Default ACL legt fest, welche Zugriffsrechte Unterobjekte dieses Verzeichnisses zum Zeitpunkt ihrer Erstellung erben. Eine Default ACL wirkt sich auf Unterverzeichnisse ebenso wie auf Dateien aus.

Auswirkungen einer Default ACL

Die Zugriffsrechte in einer Default ACL werden an Dateien und Unterverzeichnisse unterschiedlich vererbt:

- Ein Unterverzeichnis erbt die Default ACL des übergeordneten Verzeichnisses sowohl als seine eigene Default ACL als auch als Access ACL.
- Eine Datei erbt die Default ACL als ihre eigene Access ACL.

Alle Systemaufrufe (engl. *system calls*), die Dateisystemobjekte anlegen, verwenden einen `mode` Parameter. Der `mode` Parameter legt die Zugriffsrechte auf das neu anzulegende Dateisystemobjekt fest:

- Hat das übergeordnete Verzeichnis keine Default ACL, ergeben sich die Berechtigungen aus den im `mode`-Parameter angegebenen Berechtigungen, von denen die in der `umask` gesetzten Rechte abgezogen werden.
- Existiert eine Default ACL für das übergeordnete Verzeichnis, werden die Berechtigungsbits entsprechend der Schnittmenge aus dem Wert des `mode` Parameters und den in der Default ACL festgelegten Berechtigungen zusammengesetzt und dem Objekt zugewiesen. Die `umask` wird in diesem Fall nicht beachtet.

Default ACLs in der Praxis

Die drei folgenden Beispiele führen Sie an die wichtigsten Operationen an Verzeichnissen und Default ACLs heran:

- Anlegen einer Default ACL für ein bestehendes Verzeichnis
- Anlegen eines Unterverzeichnisses in einem Verzeichnis mit Default ACL
- Anlegen einer Datei in einem Verzeichnis mit Default ACL

1. Sie fügen dem schon existierenden Verzeichnis `mydir/` eine Default ACL hinzu:

   ```
   setfacl -d -m group:djungle:r-x mydir
   ```

   Die `-d` Option des `setfacl` Kommandos weist `setfacl` an, die folgenden Modifikationen (Option `-m`) auf der Default ACL vorzunehmen.

   Sehen Sie sich das Ergebnis dieses Befehls genauer an:

   ```
   getfacl mydir

   # file: mydir
   # owner: tux
   # group: projekt3
   user::rwx
   user:jane:rwx
   group::r-x
   group:djungle:rwx
   mask::rwx
   other::---
   default:user::rwx
   default:group::r-x
   default:group:djungle:r-x
   default:mask::r-x
   default:other::---
   ```

   `getfacl` liefert sowohl die Access ACL als auch die Default ACL zurück. Alle Zeilen, die mit `default` beginnen, bilden zusammen die Default ACL. Obwohl Sie dem `setfacl` Befehl lediglich einen Eintrag für die Gruppe `djungle` in die Default ACL mitgegeben hatten, hat `setfacl` automatisch alle anderen Einträge aus der Access ACL kopiert, um so eine gültige Default ACL zu bilden. Default ACLs haben keinen direkten Einfluss auf die Zugriffsberechtigungen und wirken sich nur beim Erzeugen von Dateisystemobjekten aus. Beim Vererben wird nur die Default ACL des übergeordneten Verzeichnisses beachtet.

2. Legen Sie im nächsten Beispiel mit `mkdir` ein Unterverzeichnis in `mydir/` an, welches die Default ACL „erben“ wird.

```
mkdir mydir/mysubdir
getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: projekt3
user::rwx
group::r-x
group:djungle:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:djungle:r-x
default:mask::r-x
default:other::---
```

   Wie erwartet, hat das neu angelegte Unterverzeichnis `mysubdir/` die Rechte aus der Default ACL des übergeordneten Verzeichnisses. Die Access ACL von `mysubdir/` ist ein exaktes Abbild der Default ACL von `mydir/`, ebenso die Default ACL, die dieses Verzeichnis wiederum an seine Unterobjekte weitervererben wird.

3. Legen Sie im `mydir/` Verzeichnis mit `touch` eine Datei an:

```
touch mydir/myfile
ls -l mydir/myfile

-rw-r-----+ ... tux projekt3 ... mydir/myfile

getfacl mydir/myfile

# file: mydir/myfile
# owner: tux
# group: projekt3
user::rw-
group::r-x          # effective:r--
group:djungle:r-x   # effective:r--
mask::r--
other::---
```

   Wichtig an diesem Beispiel: `touch` übergibt `mode` mit dem Wert von `0666`, das bedeutet, dass neue Dateien mit Lese- und Schreibrechten für alle Benutzerklassen angelegt werden, so nicht entweder per

`umask` oder Default ACL andere Beschränkungen existieren (siehe Abschnitt 27.3.4 auf Seite 774).

Am konkreten Beispiel heißt dies, dass alle Zugriffsrechte, die nicht im `mode` Wert enthalten sind, aus den entsprechenden ACL-Einträgen entfernt werden: Aus dem ACL-Eintrag der *group class* wurden keine Berechtigungen entfernt, allerdings wurde der *mask* Eintrag dahingehend angepasst, dass nicht per `mode` gesetzte Berechtigungsbits maskiert werden.

Auf diese Weise ist sichergestellt, dass zum Beispiel Compiler reibungslos mit ACLs interagieren können. Sie können Dateien mit beschränkten Zugriffsrechten anlegen und diese anschließend als ausführbar markieren. Über den `mask` Mechanismus ist gewährleistet, dass die richtigen Benutzer und Gruppen schließlich die Datei ausführen können.

27.3.5 Auswertung einer ACL

Nachdem Sie den Umgang mit den wichtigsten Tools zur ACL-Konfiguration bereits verstanden haben, werden Sie im Folgenden kurz an den Auswertungsalgorithmus herangeführt, den jeder Prozess oder jede Anwendung durchlaufen muss, bevor ihm Zugriff auf ein ACL-geschütztes Dateisystemobjekt gewährt werden kann.

Grundsätzlich werden die ACL-Einträge in folgender Reihenfolge untersucht: *owner*, *named user*, *owning group* oder *named group* und *other*. Über den Eintrag, der am besten auf den Prozess passt, wird schließlich der Zugang geregelt.

Komplizierter werden die Verhältnisse, wenn ein Prozess zu mehr als einer Gruppe gehört, also potentiell auch mehrere *group* Einträge passen könnten. Aus den passenden Einträgen mit den erforderlichen Rechten wird ein beliebiger ausgesucht. Für das Endresultat „Zugriff gewährt“ ist es natürlich unerheblich, welcher dieser Einträge den Ausschlag gegeben hat. Enthält keiner der passenden *group* Einträge die korrekten Rechten, gibt wiederum ein beliebiger von ihnen den Ausschlag für das Endresultat "Zugriff verweigert".

27.4 Unterstützung in Anwendungen

Wie in den vorangehenden Abschnitten beschrieben, können mit ACLs sehr anspruchsvolle Rechteszenarien umgesetzt werden, die modernen

Anwendungen gerecht werden. Das traditionelle Rechtekonzept und ACLs lassen sich geschickt miteinander vereinbaren.

Allerdings fehlt einigen wichtigen Anwendungen noch die Unterstützung für ACLs. Insbesondere auf dem Gebiet der Backup-Anwendungen gibt es mit Ausnahme des star Archivierers keine Programme, die den vollen Erhalt der ACLs sicherstellen.

Die grundlegenden Dateikommandos (`cp`, `mv`, `ls`, ...) unterstützen ACLs. Viele Editoren und Dateimanager (z.B. Konqueror) beinhalten jedoch keine ACL-Unterstützung. Beim Kopieren von Dateien mit Konqueror gehen zur Zeit noch die ACLs verloren. Wenn eine Datei mit einer Access ACL im Editor bearbeitet wird, hängt es vom Backup-Modus des verwendeten Editors ab, ob die Access ACL nach Abschluss der Bearbeitung weiterhin vorliegt:

- Schreibt der Editor die Änderungen in die Originaldatei, bleibt die Access ACL erhalten.
- Legt der Editor eine neue Datei an, die nach Abschluss der Änderungen in die alte umbenannt wird, gehen die ACLs möglicherweise verloren, es sein denn, der Editor unterstützt ACLs.

Hinweis

Weitere Informationen

Detailinformationen zu ACLs finden Sie unter den folgenden URLs
`http://sdb.suse.de/de/sdb/html/81_acl.html`
`http://acl.bestbits.at/`
und auf den Manualpages von `getfacl`, `acl` und `setfacl`.

Hinweis

Utilities zur Systemüberwachung

In diesem Kapitel werden verschiedenen Programme und Mechanismen vorgestellt, mit denen Sie den Zustand Ihres Systems untersuchen können. Weiterhin werden einige für die tägliche Arbeit nützliche Utilities mit ihren wichtigsten Optionen beschrieben.

28.1 Konventionen 780
28.2 Liste der geöffneten Dateien: lsof 780
28.3 Wer greift auf Dateien zu: fuser 781
28.4 Eigenschaften einer Datei: stat 782
28.5 Prozesse: top 782
28.6 Prozessliste: ps 783
28.7 Prozessbaum: pstree 784
28.8 Wer macht was: w 785
28.9 Speichernutzung: free 785
28.10 Kernel Ring Buffer: dmesg 786
28.11 Dateisysteme: mount, df und du 787
28.12 Das /proc Dateisystem 788
28.13 procinfo 790
28.14 PCI Resourcen: lspci 791
28.15 System Calls eines Programmlaufes: strace 792
28.16 Library Calls eines Programmlaufes: ltrace 793
28.17 Welche Library wird benötigt: ldd 794
28.18 Interprozess-Kommunikation: ipcs 794

28.1 Konventionen

Für die vorgestellten Kommandos werden jeweils beispielhafte Ausgaben dargestellt. Darin ist die erste Zeile das Kommando selbst (nach einem Dollarzeichen als Prompt). Auslassungen werden durch ein `[...]` angedeutet und lange Zeilen, soweit notwendig, umbrochen. Umbrüche langer Zeilen sind durch einen Backslash (\) angedeutet:

```
$ command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

Damit möglichst viele Utilities erwähnt werden können, ist die Darstellung kurz gehalten. Zu allen Kommandos finden Sie mehr Information in den jeweiligen Manualpages. Die meisten Kommandos verstehen auch die Option `--help`, damit erhält man eine knappe Auflistung der möglichen Optionen.

28.2 Liste der geöffneten Dateien: lsof

Um die Liste alles Dateien anzuzeigen, die der Prozess mit der Prozess-ID ⟨*PID*⟩ geöffnet hält, benutzt man die Option `-p`. Beispielsweise, um alle von der laufenden Shell benutzten Dateien anzuzeigen:

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t (totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610 /usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410 /usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393 /usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565 /usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598 /usr/lib/zsh/4.2.0/zsh/computil.so
zsh     4694   jj    0u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48               50 /dev/pts/48
```

Es wurde die spezielle Shell-Variable $$ benutzt, die als Wert die Prozess-ID der Shell hat.

Ohne Option listet `lsof` alle momentan geöffneten Dateien, in der Regel sind dies recht viele. Wir zählen:

```
$ lsof | wc -l
3749
```

Listing aller benuzten Character-Devices:

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5            45833 /dev/zero
sshd       4685    root  mem    CHR    1,5            45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5            45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5            45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1            38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

28.3 Wer greift auf Dateien zu: fuser

Unter `/mnt` sei ein Dateisystem eingehängt:

```
$ mount -l | grep /mnt
/dev/sda on /mnt type ext2 (rw,noexec,nosuid,nodev,noatime,user=jj)
```

Der Versuch, es auszuhängen, scheitert:

```
$ umount /mnt
umount: /mnt: device is busy
```

Wir untersuchen, welche Prozesse auf die Dateien im Verzeichnis `/mnt` zugreifen:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

Nach Beenden des `less` Prozesses, der in einem anderen Terminal lief, lässt sich das Dateisystem aushängen.

28.4 Eigenschaften einer Datei: stat

Zur Übersichtlichen Anzeige der Eigenschaften einer Datei wird der Befehl `stat` verwendet:

```
$ stat xml-doc.txt
  File: 'xml-doc.txt'
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Mit der Option `--filesystem` werden Eigenschaften des Dateisystems angezeigt, auf dem sich die angegebene Datei befindet:

```
 $ /usr/bin/stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

28.5 Prozesse: top

Mit dem Kommando `top` (für: *table of processes*) wird eine Liste der Prozesse angezeigt, die all 2 Sekunden erneuert wird. Das Programm wird mit der Taste ⓠ beendet. Mit der Option `-n 1` erreicht man, dass das Programm sich nach einmaliger Anzeige der Prozessliste beendet:

```
$ top -n 1
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0  820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0  100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0    0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19    0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0    0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0    0    0    0 S  0.0  0.0   0:00.71 bdflush
       [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
```

```
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Während `top` läuft, gelangt man durch Druck auf die Taste ⓕ zu einem Menü, in dem das Format der Ausgabe sehr weitgehend beeinflusst werden kann.

Um nur die Prozesse eines bestimmten Benutzers zu überwachen, kann die Option `-U` ⟨*UID*⟩, verwendet werden, wobei ⟨*UID*⟩ die User-ID des Benutzers ist. Praktisch ist die folgende Variante:

```
$ top -U $(id -u <username>)
```

28.6 Prozessliste: ps

Der Befehl `ps` erzeugt eine Liste der Prozesse. Mit der Option `r` werden nur die wirklich laufenden angezeigt:

```
$ ps r
  PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

Die Option muss tatsächlich *ohne* minus geschrieben werden. Die vielfältigen Optionen werden teilweise mit, teilweise ohne minus eingeleitet. Die Manualpage ist gut geeignet, den potentiellen Benutzer in die Flucht zu schlagen. Glücklicherweise liefert `ps --help` eine kurze Hilfsseite.

Wir kontrollieren, wieviele `emacs`-Prozesse laufen:

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Mit der Option `-p` werden Prozesse über die Prozess-ID ausgewählt:

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200
23104 ?        S      0:00 xterm -g 100x45+0+200
23334 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

28.7 Prozessbaum: pstree

Der Befehl `pstree` gibt eine Prozessliste in Baumform aus:

```
$ pstree
init-+-atd
     |-3*[automount]
     |-bdflush
     |-cron
  [...]
     |-usb-storage-1
     |-usb-storage-2
     |-10*[xterm---zsh]
     |-xterm---zsh---mutt
     |-2*[xterm---su---zsh]
     |-xterm---zsh---ssh
     |-xterm---zsh---pstree
     |-ypbind---ypbind---2*[ypbind]
     `-zsh---startx---xinit4-+-X
                             `-ctwm-+-xclock
                                    |-xload
                                    `-xosview.bin
```

Mit der Option `-p` werden die Namen durch die Prozess-ID ergänzt. Um die Kommandozeilen mitanzuzeigen, wird die Option `-a` benutzt:

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  ‘-zsh,1404
      ‘-startx,1407 /usr/X11R6/bin/startx
          ‘-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              ‘-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
                  |-xload,1450 -scale 2
                  ‘-xosview.bin,1451 +net -bat +net
```

28.8 Wer macht was: w

Mit dem Kommando `w` können Sie festellen, wer auf dem System eingeloggt ist und was er tut. Beispiel:

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -bg MistyRose1 -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

Die letzte Zeile verrät, dass der Benutzer jj eine secure shell (`ssh`) Verbindung zum Rechner `totan` aufgebaut hat.

Sollten sich Benutzer von anderen Sytemen remote eingeloggt haben, dann kann man mit der option `-f` anzeigen lassen, von welchem Rechner aus diese die Verbindung aufgebaut haben.

28.9 Speichernutzung: free

Die Nutzung des RAM wird mit dem Utility `free` untersucht. Es zeigt freien sowie benutzten Speicher (und Swap) an:

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Nützlich ist die Option `-m`, die bewirkt, dass alle Grössen in MegaByte angegeben werden:

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

Die eigentlich interessante Angabe ist in der Zeile

```
-/+ buffers/cache:        191        311
```

zu finden, hier sind die Nutzung durch Buffer und Cache herausgerechnet.

Mit der Option `-d` ⟨*delay*⟩ wird die Ausgabe alle ⟨*delay*⟩ Sekunden wiederholt: `free -d 1.5` gibt alle 1,5 Sekunden die aktuellen Werte aus.

28.10 Kernel Ring Buffer: dmesg

Der Linux Kernel hält eine gewissen Menge seiner Meldungen in einem Ring Buffer vor. Mit dem Kommando `dmesg` werden diese Meldungen ausgegeben:

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
```

```
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

Die vorletzte Zeile deutet auf ein temporäres Problem des NFS-Servers `totan` hin. Die Zeilen bis dahin sind ausgelöst durch Anstecken eines USB Memory-Stick.

Weiter zurückliegende Ereignisse sind in den Dateien `/var/log/messages` und `/var/log/warn` protokolliert.

28.11 Dateisysteme: mount, df und du

Mittels `mount` stellt man fest, welches Dateisystem (Device und Typ) an welcher Stelle (Mount Point) eingehängt ist:

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

Die summarische Nutzung der Dateisysteme kann mit `df` abgefragt werden. Die Option `-h` (alias `--human-readable`) macht die Ausgabe lesbar für (normale) Menschen:

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Die Nutzer des NFS-Fileservers `totan` sollten ihre Home-Verzeichnisse alsbald aufräumen.

Die Gesamtgrösse aller Dateien unterhalb eines Verzeichnisses lässt sich mit dem Kommando `du` ermitteln. Die Option `-s` unterdrückt die Ausgabe der detaillierten Ausgabe, `-h` bewirkt wieder Menschen-Lesbarkeit.

Mittels

```
$ du -sh ~
361M    /suse/jj
```

kann man feststellen, wieviel Platz das eigene Home-Verzeichnis beansprucht.

28.12 Das /proc Dateisystem

Das `/proc` Dateisystem ist ein Pseudo-Dateisystem, in dem der Kernel wichtige Informationen in Form von virtuellen Dateien vorhält. Beispielsweise kann der Typ der CPU einfach wie folgt festgestellt werden:

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

Belegung und Verwendung der Interrupts:

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
```

```
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Einige wichtige Dateien und die enthaltenen Informationen sind:

- `/proc/devices`: verfügbare Devices
- `/proc/modules`: geladene Kernel-Module
- `/proc/cmdline`: Kernel-Kommandozeile
- `/proc/meminfo`: Detaillierte Information über Speichernutzung
- `/proc/config.gz`: `gzip`-komprimierte Konfigurationsdatei des aktuell laufenden Kernels.

Weitere Informationen finden Sie der Textdatei: `/usr/src/linux/Documentation/filesystems/proc.txt` Die Nutzung des Speichers wird mit dem Kommando `vmstat` abgefragt.

Informationen über ablaufende Prozesse befinden sich in den directories `/proc/`⟨*NNN*⟩ wobei ⟨*NNN*⟩ die Prozess-ID (PID) des jeweiligen Prozeses ist. Unter `/proc/self/` findet ein Prozess immer seine eigenen Eigenschaften:

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

In der Datei `maps` findet man die Adresszuordnung von Executables und Libraries:

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

28.13 procinfo

Wichtige Informationen aus dem `/proc`-Dateisystem werden vom Programm `procinfo` zusammengefasst:

```
$ procinfo
Linux 2.4.21-144-athlon (root@i386.suse.de) (gcc 3.3.1 ) #1 \
   Fri Nov 28 01:14:40 UTC 2003 1CPU [nunez.suse.de]

Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:        514736      496088       18648           0       56128      224656
Swap:      1794736      104488     1690248

Bootup: Wed Feb 25 09:44:25 2004    Load average: 0.00 0.01 0.00 1/104 21285

user  :       4:34:59.40   0.3%  page in : 11320141  disk 1:   474842r  358260w
nice  :       0:07:12.64   0.0%  page out: 14495036  disk 2:   649679r  989842w
system:       1:15:00.55   0.1%  swap in :    58942  disk 3:     6547r     610w
idle  :  61d 22:40:40.26  99.6%  swap out:   149085  disk 4:     1169r      23w
uptime:  62d  4:37:52.84         context :767431068

irq  0: 537347285 timer                 irq 10:     13970 usb-uhci, usb-uhci
irq  1:    814562 keyboard              irq 11: 146415669 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]           irq 12:   8008998 PS/2 Mouse
irq  6:         2                       irq 14:   2463408 ide0
irq  8:         2 rtc                   irq 15:      1355 ide1
```

Um „alle“ Informationen zu sehen, benutzen Sie die Option `-a`. Mit der Option `-n`⟨*N*⟩ werden die Informationen alle ⟨*N*⟩ Sekunden neu abgefragt. In diesem Fall muss das Programm mit der Taste ⓠ beendet werden.

Standardmäßig werden die kumulativen Werte angezeigt, mit der Option `-d` werden die differentiellen Werte angezeigt: `procinfo -dn5` zeigt die in jeweils 5 Sekunden aufgetretenen Werte an:

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer               irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard            irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]         irq 12:       132 PS/2 Mouse
irq  6:         0                     irq 14:         0 ide0
irq  8:         0 rtc                 irq 15:         0 ide1
irq  9:         0 acpi
```

28.14 PCI Resourcen: lspci

Das Kommando `lspci` listet die PCI-Resourcen:

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \
    DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
    PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
    VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
    MGA G550 AGP (rev 01)
```

Mit der Option `-v` wird das Listing ausführlicher:

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
    (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
```

```
Memory at d8000000 (32-bit, prefetchable) [size=32M]
Memory at da000000 (32-bit, non-prefetchable) [size=16K]
Memory at db000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at <unassigned> [disabled] [size=128K]
Capabilities: <available only to root>
```

Die „Namensauflösung“ der Devices erfolgt mit der Datei `/usr/share/pci.ids`. PCI-IDs, die in dieser Dile nicht gelistet sind, werden mit „Unknown device“ angezeigt.

Mit `-vv` erhält man alle Informationen, die überhaupt vom Programm abgefragt werden können. Die reinen numerischen Werte werden mit der Option `-n` angezeigt.

28.15 System Calls eines Programmlaufes: strace

Sämtliche System Calls eines laufenden Prozesses kann man mit dem Utility `strace` verfolgen. Man gibt das Kommando wie gewohnt an, ergänzt durch ein `strace` am Beginn der Zeile:

```
$ strace ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
        = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
        = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Um beispielsweise alle Versuche, eine Datei zu öffnen, zu verfolgen, verfährt man wie folgt:

```
$ strace ls myfile.txt 2>&1 | grep open
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT
 (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/librt.so.1", O_RDONLY)       = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libc.so.6", O_RDONLY)        = 3
open("/lib/libpthread.so.0", O_RDONLY)  = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
```

Um auch alle Kindprozesse zu verfolgen, benutzt man die Option `-f`. Das Verhalten und Ausgabeformat von strace lassen sich sehr weitgehend kontrollieren, siehe dazu `man strace`.

28.16 Library Calls eines Programmlaufes: ltrace

Die Library Calls eines Prozesses lassen sich mit dem Kommando `ltrace` verfolgen. Die Benutzung ist grundsätzlich wie bei `strace`. Mit der Option `-c` wird die Anzahl und Dauer der erfolgten Library Calls ausgegeben:

```
$ strace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

28.17 Welche Library wird benötigt: ldd

Mittels `ldd` findet man heraus, welche Libraries das als Argument angegebene dynamische Executable nachladen würde:

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Statische Binaries benötigen keine dynamischen Libraries (Überraschung!):

```
$ ldd /bin/rpm
        not a dynamic executable
$ file /bin/rpm
/bin/rpm: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
      statically linked, stripped
```

28.18 Interprozess-Kommunikation: ipcs

Mit dem Kommunikation `ipcs` erhält man eine Auflistung der benutzten IPC Resourcen:

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

Teil V

Anhang

Informationsquellen und Dokumentationen

Dieses Kapitel zeigt Ihnen, wo Sie Informationen und Dokumentationen zu Ihrem System finden können.

SUSE-Dokumentationen

Umfangreiche Informationen dazu finden Sie in unseren Büchern im HTML- oder PDF-Format erhalten in den RPM-Paketen `suselinux-adminguide_en` und `suselinux-adminguide_en-pdf`).

Bei einer Standardinstallation werden die Bücher im Verzeichnis `/usr/share/doc/manual/` installiert. Mit Hilfe des SUSEHelpCenters haben Sie Zugriff auf diese Informationen.

Das Linux Documentation Projekt (TLDP)

Das Linux Documentation Projekt (siehe `http://www.tldp.org/`) ist ein Team von Freiwilligen, die Dokumentation über Linux erstellen. TLDP enthält HOWTOs, FAQs und sog. Guides (Handbücher), die alle unter einer freien Lizenz veröffentlicht wurden.

HOWTOs sind Schritt-für-Schritt-Anleitungen und richten sich an Endbenutzer, Systemadministratoren oder Programmierer. Zum Beispiel wird das Einrichten eines DHCP-Servers in einem HOWTO beschrieben und was es zu beachten gibt, nicht jedoch wie Linux als solches installiert wird. In der

Regel sind solche Dokumentationen recht allgemein gehalten, damit sie auf jede Distribution anwendbar sind. Das Paket `howto` enthält HOWTOs in ASCII. Anwender, die HTML bevorzugen, sollten `howtoenh` installieren.

FAQs (engl. *Frequently Asked Questions*) sind Sammlungen von Fragen und Antworten zu bestimmten Problemfeldern, die häufig in Mailinglisten öfters gestellt werden. Zum Beispiel „Was ist LDAP?“, „Was ist ein RAID?“ usw. Texte dieser Kategorie sind im Allgemeinen recht kurz.

Guides sind Bücher, die ein Thema wesentlich detaillierter behandeln können als dies HOWTOs und FAQs tun. Beispiele sind Kernelprogrammierung, Netzwerkadministration u. a. Die Absicht dahinter ist, dem Leser einen fundierten Wissenstand zu vermitteln.

Manche Dokumentationen des TLDP sind auch in anderen Formaten verfügbar, wie zum Beispiel PDF, einzelne und multiple HTML-Seiten, PostScript und als SGML/XML-Quellen. Teilweise gibt es auch Übersetzungen in verschiedene Sprachen.

Man- und Infopages

Eine Manpage (engl. *Manual page*) ist ein Hilfstext zu einem Befehl, Systemaufruf, Dateiformat o. ä. Für gewöhnlich wird eine Manpage in unterschiedliche Sektionen unterteilt wie Name, Syntax, Beschreibung, Optionen, Dateien, usw.

Um eine Manpage darzustellen, geben Sie ein:

```
man ls
```

Die vorige Eingabe zeigt den Hilfstext zum Befehl `ls` an. Mit den Cursor-Tasten können Sie den sichtbaren Bereich verschieben, mit ⓠ verlassen Sie `man`. Um eine Manpage zu drucken (zum Beispiel für den Befehl `ls`), geben Sie ein:

```
card ls
```

Weitere Hilfe zum Befehl `card` (Paket `a2ps`) gibt es mit der Option `--help`.

Manche Dokumentation ist auch im Info-Format verfügbar, zum Beispiel `grep`. Der Aufruf lautet:

```
info grep
```

Im Gegensatz zu Manpages sind Infopages ausführlicher und in verschiedene „Knoten“ aufgeteilt. Ein Knoten stellt dabei eine Seite dar, die ähnlich wie ein HTML-Browser mit einem Info Reader gelesen werden kann. Um in einer Infopage zu navigieren, verwendet man die Tasten ⓟ (previous, vorherige Seite) und ⓝ (next, nächste Seite). Mit ⓠ verlassen Sie `info`. Weitere Tasten finden Sie in der Dokumentation zu `info` (rufen Sie `info info` auf).

Sowohl Man- als auch Infopages lassen sich im Konqueror durch Eingabe von `man:`⟨*`Befehl`*⟩ bzw. `info:`⟨*`Befehl`*⟩ in der URL-Zeile aufrufen.

Standards und Spezifikationen

Falls Sie Informationen über Standards oder Spezifikationen benötigen, gibt es hierfür verschiedene Informationsmöglichkeiten:

`http://www.w3.org` Das *World Wide Web Consortium* (W3C) ist wohl eine der bekanntesten Einrichtungen, wurde im Oktober 1994 von TIM BERNERS-LEE gegründet und konzentriert sich auf die Standardisierung von Web-Technologien. Es fördert die Verbreitung von offenen, lizenzfreien und herstellerunabhängigen Spezifikationen wie zum Beispiel HTML, XHTML, XML und anderen. Diese „Web-Standards“ werden in einem 4-stufigen Prozess in sog. *Working Groups* entwickelt und als *W3C Recommendation (REC)* der Öffentlichkeit vorgestellt.

`http://www.oasis-open.org` OASIS (*Organization for the Advancement of Structured Information Standards*) ist ein internationales Konsortium, das sich auf die Entwicklung von Standards zur Web-Sicherheit, E-Business, Geschäftstransaktionen, Logistik und der Interoperabilität zwischen verschiedenen Märkten spezialisiert hat.

`http://www.ietf.org` Die *Internet Engineering Task Force* (IETF) ist eine international agierende Gemeinschaft von Forschern, Netzwerkdesignern, Lieferanten und Anwendern. Sie konzentriert sich auf die Entwicklung der Internet-Architektur und des reibungslosen Betrieb des Internets durch Protokolle.

Jeder IETF-Standard wird als RFC (*Request for Comments*, siehe `http://www.ietf.org/rfc.html`) veröffentlicht und ist gebührenfrei. Es gibt sechs Arten von RFCs: propsed standards, draft standards, Internet standards, experimental protocols, Informational documents und historic standards. Nur die ersten drei (proposed,

draft, and full) sind IETF-Standards im engeren Sinne (siehe hierzu auch die Zusammenfassung unter `http://www.ietf.org/rfc/rfc1796.txt`).

`http://www.ieee.org` Das *Institute of Electrical and Electronics Engineers* (IEEE) ist eine Einrichtung, die Standards in den Bereichen Informationstechnologie, Telekommunikation, Medizin und Gesundheitspflege, Transportwesen u. a. erstellt. IEEE-Standards sind kostenpflichtig.

`http://www.iso.org` Das ISO-Kommittee (*Internationl Organization for Standards*) ist der weltgrößte Entwickler von Standards und unterhält ein Netzwerk von nationalen Standardisierungsinstituten in über 140 Ländern. ISO-Standards sind kostenpflichtig.

`http://www.din.de`, `http://www.din.com`
Das Deutsches Institut für Normung (DIN) ist ein eingetragener, technisch-wissenschaftlicher Verein und wurde 1917 gegründet. Laut DIN ist es „für die Normungsarbeit zuständige Institution in Deutschland und vertritt die deutschen Interessen in den weltweiten und europäischen Normungsorganisationen".

Der Verein ist ein Zusammenschluss von Herstellern, Verbrauchern, Handwerkern, Dienstleistungsunternehmen, Wissenschaftlern und anderen Personen, die ein Interesse an der Erstellung von Normen haben. Die Normen sind kostenpflichtig und können über die Homepage von DIN bestellt werden.

Manual-Page von e2fsck

E2FSCK(8) E2FSCK(8)

NAME
e2fsck - check a Linux second extended file system

SYNOPSIS
e2fsck [-pacnyrdfvstDFSV] [-b superblock] [-B block size] [-l|-L bad_blocks_file] [-C fd] [-j external-journal] [-E extended_options] device

DESCRIPTION
e2fsck is used to check a Linux second extended file sys tem (ext2fs). E2fsck also supports ext2 filesystems coun taining a journal, which are also sometimes known as ext3 filesystems, by first applying the journal to the filesys tem before continuing with normal e2fsck processing. After the journal has been applied, a filesystem will nor mally be marked as clean. Hence, for ext3 filesystems, e2fsck will normally run the journal and exit, unless its superblock indicates that further checking is required.

device is the device file where the filesystem is stored (e.g. /dev/hdc1).

OPTIONS
-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock
Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the

backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize
Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode. If this option is specified twice, then the bad block scan will be done using a non-destructive read-write test.

-C fd This option causes e2fsck to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by pro grams which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a com pletion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging e2fsck).

-D Optimize directories in filesystem. This option causes e2fsck to try to optimize all directories, either by reindexing them if the filesystem sup ports directory indexing, or by sorting and com

pressing directories for smaller directories, or for filesystems using traditional linear directo ries.

-E extended_options
Set e2fsck extended options. Extended options are comma separated, and may take an argument using the equals ('=') sign. The following options are sup ported:

ea_ver=extended_attribute_version
Assume the format of the extended attribute blocks in the filesystem is the specified version number. The ver sion number may be 1 or 2. The default extended attribute version format is 2.

-f Force checking even if the file system seems clean.

-F Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
Set the pathname where the external-journal for this filesystem can be found.

-l filename
Add the block numbers listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program. Note that the block num bers are based on the blocksize of the filesystem. Hence, badblocks(8) must be given the blocksize of the filesystem in order to obtain correct results. As a result, it is much simpler and safer to use the -c option to e2fsck, since it will assure that the correct parameters are passed to the badblocks program.

-L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

-n Open the filesystem read-only, and assume an answer of 'no' to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However,

no other changes will be made to the filesystem.)

-p Automatically repair ("preen") the file system without any questions.

-r This option does nothing at all; it is provided only for backwards compatibility.

-s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesys tem is already in the standard byte-order, e2fsck will take no action.

-S This option will byte-swap the filesystem, regard less of its current byte-order.

-t Print timing statistics for e2fsck. If this option is used twice, additional timing statistics are printed on a pass by pass basis.

-v Verbose mode.

-V Print version information and exit.

-y Assume an answer of ‘yes’ to all questions; allows e2fsck to be used non-interactively.

EXIT CODE

The exit code returned by e2fsck is the sum of the follow ing conditions:

0 - No errors
1 - File system errors corrected
2 - File system errors corrected, system should be rebooted
4 - File system errors left uncorrected
8 - Operational error
16 - Usage or syntax error
32 - E2fsck canceled by user request
128 - Shared library error

SIGNALS

The following signals have the following effect when sent to e2fsck.

SIGUSR1

This signal causes e2fsck to start displaying a completion bar. (See discussion of the -C option.)

SIGUSR2

This signal causes e2fsck to stop displaying a com pletion bar.

REPORTING BUGS

Almost any piece of software will have bugs. If you manage to find a filesystem which causes e2fsck to crash, or which e2fsck is unable to repair, please report it to the author.

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trou ble, try running the debugfs(8) command and send the out put of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuen code(1).

Always include the full version string which e2fsck dis plays when it is run, so I know which version you are run ning.

AUTHOR

This version of e2fsck was written by Theodore Ts'o <tytso@mit.edu>.

SEE ALSO

mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)

E2fsprogs version 1.34 July 2003 E2FSCK(8)

Manual-Page von reiserfsck

REISERFSCK(8) REISERFSCK(8)

NAME

reiserfsck - check a Linux Reiserfs file system

SYNOPSIS

reiserfsck [-afprVy] [--rebuild-sb | --check | --fix-fixable | --rebuild-tree | --clean-attributes] [-j | --journal device] [-z | --adjust-size] [-n | --nolog] [-l | --logfile file] [-q | --quiet] [-y | --yes] [-S | --scan-whole-partition] [--no-journal-available] device

DESCRIPTION

Reiserfsck searches for a Reiserfs filesystem on a device, replays any necessary transactions, and either checks or repairs the file system.

device is the special file corresponding to the device or partition (e.g /dev/hdXX for IDE disk partition or /dev/sdXX for SCSI disk partition).

OPTIONS

--rebuild-sb

This option recovers the superblock on a Reiserfs partition. Normally you only need this option if mount reports "read_super_block: can't find a reis erfs file system" and you are sure that a Reiserfs file system is there.

--check
This default action checks file system consistency and reports but does not repair any corruption that it finds. This option may be used on a read-only file system mount.

--fix-fixable
This option recovers certain kinds of corruption that do not require rebuilding the entire file sys tem tree (--rebuild-tree). Normally you only need this option if the --check option reports "corrup tion that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, cor recting st_size and st_blocks for directories, and deleting invalid directory entries.

--rebuild-tree
This option rebuilds the entire file system tree using leaf nodes found on the device. Normally you only need this option if the --check option reports "corruption that can be fixed only during --rebuild-tree". You are strongly encouraged to make a backup copy of the whole partition before attempting the --rebuild-tree option.

--clean-attributes
This option cleans reserved fields of Stat-Data items.

--journal device , -j device
This option supplies the device name of the current file system journal. This option is required when the journal resides on a separate device from the main data device (although it can be avoided with the expert option --no-journal-available).

--adjust-size, -z
This option causes reiserfsck to correct file sizes that are larger than the offset of the last discov ered byte. This implies that holes at the end of a file will be removed. File sizes that are smaller than the offset of the last discovered byte are corrected by --fix-fixable.

```
       --logfile file, -l  file
              This option causes reiserfsck to report any corrup
              tion it finds to the specified log file rather than
              stderr.

       --nolog, -n
              This option prevents reiserfsck from reporting  any
              kinds of corruption.

       --quiet, -q
              This  option prevents reiserfsck from reporting its
              rate of progress.

       --yes, -y
              This option inhibits reiserfsck from asking you for
              confirmation  after telling you what it is going to
              do, assuming yes. For safety, it does not work with
              the --rebuild-tree option.

       -a, -p These  options are usually passed by fsck -A during
              the automatic checking of those  partitions  listed
              in  /etc/fstab.  These  options cause reiserfsck to
              print some information  about  the  specified  file
              system,  check if error flags in the superblock are
              set and  do  some  light-weight  checks.  If  these
              checks reveal a corruption or the flag indicating a
              (possibly fixable) corruption is found set  in  the
              superblock,  then  reiserfsck  switches to the fix-
              fixable mode. If the flag indicating a  fatal  cor
              ruption  is found set in the superblock, then reis
              erfsck finishes with an error.

       -V     This option prints the  reiserfsprogs  version  and
              exit.

       -r, -f These options are ignored.

EXPERT OPTIONS
       DO  NOT  USE  THESE  OPTIONS  UNLESS YOU KNOW WHAT YOU ARE
       DOING.  WE ARE NOT RESPONSIBLE  IF  YOU  LOSE  DATA  AS  A
       RESULT OF THESE OPTIONS.

       --no-journal-available
              This  option  allows reiserfsck to proceed when the
              journal device is not available. This option has no
```

effect when the journal is located on the main data device. NOTE: after this operation you must use reiserfstune to specify a new journal device.

--scan-whole-partition, -S
This option causes --rebuild-tree to scan the whole partition, not only used space on the partition.

EXAMPLE OF USING

1. You think something may be wrong with a reiserfs partition on /dev/hda1 or you would just like to perform a periodic disk check.

2. Run reiserfsck --check --logfile check.log /dev/hda1. If reiserfsck --check exits with status 0 it means no errors were discovered.

3. If reiserfsck --check exits with status 1 (and reports about fixable corruptions) it means that you should run reiserfsck --fix-fixable --logfile fixable.log /dev/hda1.

4. If reiserfsck --check exits with status 2 (and reports about fatal corruptions) it means that you need to run reiserfsck --rebuild-tree. If reiserfsck --check fails in some way you should also run reiserfsck --rebuild-tree, but we also encourage you to submit this as a bug report.

5. Before running reiserfsck --rebuild-tree, please make a backup of the whole partition before proceeding. Then run reiserfsck --rebuild-tree --logfile rebuild.log /dev/hda1.

6. If the --rebuild-tree step fails or does not recover what you expected, please submit this as a bug report. Try to provide as much information as possible and we will try to help solve the problem.

EXIT CODES

reiserfsck uses the following exit codes:

0 - No errors.
1 - File system errors corrected.
4 - File system fatal errors left uncorrected, reiserfsck --rebuild-tree needs to be launched.
6 - File system fixable errors left uncorrected, reiserfsck --fix-fixable needs to be launched.
8 - Operational error.

```
          16 - Usage or syntax error.

AUTHOR
       This version of reiserfsck  has  been  written  by  Vitaly
       Fertman <vitaly@namesys.com>.

BUGS
       There  are  likely  to be some bugs. Please report bugs to
       the ReiserFS mail-list <reiserfs-list@namesys.com>.

TODO
       Faster recovering, signal handling,  i/o  error  handling,
       etc.

SEE ALSO
       mkreiserfs(8),  reiserfstune(8)  resize_reiserfs(8), debu
       greiserfs(8),

Reiserfsprogs-3.6.9         April 2003              REISERFSCK(8)
```

D

Deutsche Übersetzung der GNU General Public License

Der folgende Text folgt im Wesentlichen der inoffiziellen Übersetzung von Katja Lachmann und der Überarbeitung von Peter Gerwinski (31. Oktober 1996, 4. Juni 2000).

Diese Übersetzung wird mit der Absicht angeboten, das Verständnis der *GNU General Public License* (GNU-GPL) zu erleichtern. Es handelt sich jedoch nicht um eine offizielle oder im rechtlichen Sinne anerkannte Übersetzung.

Die *Free Software Foundation* (FSF) ist nicht der Herausgeber dieser Übersetzung, und sie hat diese Übersetzung auch nicht als rechtskräftigen Ersatz für die Original-GNU-GPL (siehe `http://www.gnu.org/copyleft/gpl.html`) anerkannt. Da die Übersetzung nicht sorgfältig von Anwälten überprüft wurde, können die Übersetzer nicht garantieren, dass die Übersetzung die rechtlichen Aussagen der GNU-GPL exakt wiedergibt. Wenn Sie sichergehen wollen, dass von Ihnen geplante Aktivitäten im Sinne der GNU-GPL gestattet sind, halten Sie sich bitte an die englischsprachige Originalversion.

Die *Free Software Foundation* möchte Sie darum bitten, diese Übersetzung nicht als offizielle Lizenzbedingungen für von Ihnen geschriebene Programme zu verwenden. Bitte benutzen Sie hierfür stattdessen die von der *Free Software Foundation* herausgegebene englischsprachige Originalversion.

This is a translation of the GNU General Public License into German. This translation is distributed in the hope that it will facilitate understanding, but it is not an official or legally approved translation.

The Free Software Foundation is not the publisher of this translation and has not approved it as a legal substitute for the authentic GNU General Public License. The translation has not been reviewed carefully by lawyers, and therefore the translator cannot be sure that it exactly represents the legal meaning of the GNU General Public License. If you wish to be sure whether your planned activities are permitted by the GNU General Public License, please refer to the authentic English version.

The Free Software Foundation strongly urges you not to use this translation as the official distribution terms for your programs; instead, please use the authentic English version published by the Free Software Foundation.

GNU General Public License

Deutsche Übersetzung der Version 2, Juni 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Es ist jedermann gestattet, diese Lizenzurkunde zu vervielfältigen und unveränderte Kopien zu verbreiten; Änderungen sind jedoch nicht erlaubt.

Hinweis

Diese Übersetzung ist kein rechtskräftiger Ersatz für die englischsprachige Originalversion!

Hinweis

Vorwort

Die meisten Softwarelizenzen sind daraufhin entworfen worden, Ihnen die Freiheit zu nehmen, die Software weiterzugeben und zu verändern. Im Gegensatz dazu soll Ihnen die *GNU General Public License*, die Allgemeine Öffentliche GNU-Lizenz, ebendiese Freiheit garantieren. Sie soll sicherstellen, dass die Software für alle Benutzer frei ist. Diese Lizenz gilt für den Großteil der von der *Free Software Foundation* herausgegebenen Software und für alle anderen Programme, deren Autoren ihr Datenwerk dieser Lizenz unterstellt haben. Auch Sie können diese Möglichkeit der Lizenzierung für Ihre Programme anwenden. (Ein anderer Teil der Software der *Free Software Foundation* unterliegt stattdessen der *GNU Library General Public License*, der Allgemeinen Öffentlichen GNU-Lizenz für Bibliotheken. – Mittlerweile

wurde die GNU Library Public License von der GNU Lesser Public License abgelöst.)

Die Bezeichnung *„freie" Software* bezieht sich auf Freiheit, nicht auf den Preis. Unsere Lizenzen sollen Ihnen die Freiheit garantieren, Kopien freier Software zu verbreiten (und etwas für diesen Service zu berechnen, wenn Sie möchten), die Möglichkeit, die Software im Quelltext zu erhalten oder den Quelltext auf Wunsch zu bekommen. Die Lizenzen sollen garantieren, dass Sie die Software ändern oder Teile davon in neuen freien Programmen verwenden dürfen – und dass Sie wissen, dass Sie dies alles tun dürfen.

Um Ihre Rechte zu schützen, müssen wir Einschränkungen machen, die es jedem verbieten, Ihnen diese Rechte zu verweigern oder Sie aufzufordern, auf diese Rechte zu verzichten. Aus diesen Einschränkungen folgen bestimmte Verantwortlichkeiten für Sie, wenn Sie Kopien der Software verbreiten oder sie verändern.

Beispielsweise müssen Sie den Empfängern alle Rechte gewähren, die Sie selbst haben, wenn Sie – kostenlos oder gegen Bezahlung – Kopien eines solchen Programms verbreiten. Sie müssen sicherstellen, dass auch die Empfänger den Quelltext erhalten bzw. erhalten können. Und Sie müssen ihnen diese Bedingungen zeigen, damit sie ihre Rechte kennen.

Wir schützen Ihre Rechte in zwei Schritten: (1) Wir stellen die Software unter ein Urheberrecht (Copyright), und (2) wir bieten Ihnen diese Lizenz an, die Ihnen das Recht gibt, die Software zu vervielfältigen, zu verbreiten und/oder zu verändern.

Um die Autoren und uns zu schützen, wollen wir darüberhinaus sicherstellen, dass jeder erfährt, dass für diese freie Software keinerlei Garantie besteht. Wenn die Software von jemand anderem modifiziert und weitergegeben wird, möchten wir, dass die Empfänger wissen, dass sie nicht das Original erhalten haben, damit irgendwelche von anderen verursachte Probleme nicht den Ruf des ursprünglichen Autors schädigen.

Schließlich und endlich ist jedes freie Programm permanent durch Software-Patente bedroht. Wir möchten die Gefahr ausschließen, dass Distributoren eines freien Programms individuell Patente lizenzieren -- mit dem Ergebnis, dass das Programm proprietär würde. Um dies zu verhindern, haben wir klargestellt, dass jedes Patent entweder für freie Benutzung durch jedermann lizenziert werden muss oder überhaupt nicht lizenziert werden darf.

Es folgen die genauen Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung.

Allgemeine Öffentliche GNU-Lizenz

Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung

0. Diese Lizenz gilt für jedes Programm und jedes andere Datenwerk, in dem ein entsprechender Vermerk des Copyright-Inhabers darauf hinweist, dass das Datenwerk unter den Bestimmungen dieser *General Public License* verbreitet werden darf. Im Folgenden wird jedes derartige Programm oder Datenwerk als „das Programm" bezeichnet; die Formulierung „auf dem Programm basierendes Datenwerk" bezeichnet das Programm sowie jegliche Bearbeitung des Programms im urheberrechtlichen Sinne, also ein Datenwerk, welches das Programm, auch auszugsweise, sei es unverändert oder verändert und/oder in eine andere Sprache übersetzt, enthält. (Im Folgenden wird die Übersetzung ohne Einschränkung als „Bearbeitung" eingestuft.) Jeder Lizenznehmer wird im Folgenden als „Sie" angesprochen.

Andere Handlungen als Vervielfältigung, Verbreitung und Bearbeitung werden von dieser Lizenz nicht berührt; sie fallen nicht in ihren Anwendungsbereich. Der Vorgang der Ausführung des Programms wird nicht eingeschränkt, und die Ausgaben des Programms unterliegen dieser Lizenz nur, wenn der Inhalt ein auf dem Programm basierendes Datenwerk darstellt (unabhängig davon, dass die Ausgabe durch die Ausführung des Programmes erfolgte). Ob dies zutrifft, hängt von den Funktionen des Programms ab.

1. Sie dürfen auf beliebigen Medien unveränderte Kopien des Quelltextes des Programms, wie sie ihn erhalten haben, anfertigen und verbreiten. Voraussetzung hierfür ist, dass Sie mit jeder Kopie einen entsprechenden Copyright-Vermerk sowie einen Haftungsausschluss veröffentlichen, alle Vermerke, die sich auf diese Lizenz und das Fehlen einer Garantie beziehen, unverändert lassen und des Weiteren allen anderen Empfängern des Programms zusammen mit dem Programm eine Kopie dieser Lizenz zukommen lassen.

Sie dürfen für den eigentlichen Kopiervorgang eine Gebühr verlangen. Wenn Sie es wünschen, dürfen Sie auch gegen Entgelt eine Garantie für das Programm anbieten.

2. Sie dürfen Ihre Kopie(n) des Programms oder einen Teil davon verändern, wodurch ein auf dem Programm basierendes Datenwerk entsteht; Sie dürfen derartige Bearbeitungen unter den Bestimmungen von Paragraph 1

vervielfältigen und verbreiten, vorausgesetzt, dass zusätzlich alle im Folgenden genannten Bedingungen erfüllt werden:

1. Sie müssen die veränderten Dateien mit einem auffälligen Vermerk versehen, der auf die von Ihnen vorgenommene Modifizierung und das Datum jeder Änderung hinweist.

2. Sie müssen dafür sorgen, dass jede von Ihnen verbreitete oder veröffentlichte Arbeit, die ganz oder teilweise von dem Programm oder Teilen davon abgeleitet ist, Dritten gegenüber als Ganzes unter den Bedingungen dieser Lizenz ohne Lizenzgebühren zur Verfügung gestellt wird.

3. Wenn das veränderte Programm normalerweise bei der Ausführung interaktiv Kommandos einliest, müssen Sie dafür sorgen, dass es, wenn es auf dem üblichsten Wege für solche interaktive Nutzung gestartet wird, eine Meldung ausgibt oder ausdruckt, die einen geeigneten Copyright-Vermerk enthält sowie einen Hinweis, dass es keine Gewährleistung gibt (oder anderenfalls, dass Sie Garantie leisten), und dass die Benutzer das Programm unter diesen Bedingungen weiter verbreiten dürfen. Auch muss der Benutzer darauf hingewiesen werden, wie er eine Kopie dieser Lizenz ansehen kann. (Ausnahme: Wenn das Programm selbst interaktiv arbeitet, aber normalerweise keine derartige Meldung ausgibt, muss Ihr auf dem Programm basierendes Datenwerk auch keine solche Meldung ausgeben.)

Diese Anforderungen gelten für das bearbeitete Datenwerk als Ganzes. Wenn identifizierbare Teile des Datenwerkes nicht von dem Programm abgeleitet sind und vernünftigerweise als unabhängige und eigenständige Datenwerke für sich selbst zu betrachten sind, dann gelten diese Lizenz und ihre Bedingungen nicht für die betroffenen Teile, wenn Sie diese als eigenständige Datenwerke weitergeben. Wenn Sie jedoch dieselben Abschnitte als Teil eines Ganzen weitergeben, das ein auf dem Programm basierendes Datenwerk darstellt, dann muss die Weitergabe des Ganzen nach den Bedingungen dieser Lizenz erfolgen, deren Bedingungen für weitere Lizenznehmer somit auf das gesamte Ganze ausgedehnt werden – und somit auf jeden einzelnen Teil, unabhängig vom jeweiligen Autor.

Somit ist es nicht die Absicht dieses Abschnittes, Rechte für Datenwerke in Anspruch zu nehmen oder Ihnen die Rechte für Datenwerke streitig zu machen, die komplett von Ihnen geschrieben wurden; vielmehr ist es die Absicht, die Rechte zur Kontrolle der Verbreitung von Datenwerken, die auf dem Programm basieren oder unter seiner auszugsweisen Verwendung zusammengestellt worden sind, auszuüben.

Ferner bringt auch das einfache Zusammenlegen eines anderen Datenwerkes, das nicht auf dem Programm basiert, mit dem Programm oder einem auf dem Programm basierenden Datenwerk auf ein- und demselben Speicher- oder Vertriebsmedium dieses andere Datenwerk nicht in den Anwendungsbereich dieser Lizenz.

3. Sie dürfen das Programm (oder ein darauf basierendes Datenwerk gemäß Paragraph 2) als Objectcode oder in ausführbarer Form unter den Bedingungen der Paragraphen 1 und 2 kopieren und weitergeben – vorausgesetzt, dass Sie außerdem eine der folgenden Leistungen erbringen:

1. Liefern Sie das Programm zusammen mit dem vollständigen zugehörigen maschinenlesbaren Quelltext auf einem für den Datenaustausch üblichen Medium aus, wobei die Verteilung unter den Bedingungen der Paragraphen 1 und 2 erfolgen muss. Oder:
2. Liefern Sie das Programm zusammen mit einem mindestens drei Jahre lang gültigen schriftlichen Angebot aus, jedem Dritten eine vollständige maschinenlesbare Kopie des Quelltextes zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen – wobei der Quelltext unter den Bedingungen der Paragraphen 1 und 2 auf einem für den Datenaustausch üblichen Medium weitergegeben wird. Oder:
3. Liefern Sie das Programm zusammen mit dem schriftlichen Angebot der Zurverfügungstellung des Quelltextes aus, das Sie selbst erhalten haben. (Diese Alternative ist nur für nicht-kommerzielle Verbreitung zulässig und nur, wenn Sie das Programm als Objectcode oder in ausführbarer Form mit einem entsprechenden Angebot gemäß Absatz 2 erhalten haben.)

Unter dem Quelltext eines Datenwerkes wird diejenige Form des Datenwerkes verstanden, die für Bearbeitungen vorzugsweise verwendet wird. Für ein ausführbares Programm bedeutet „der komplette Quelltext“: Der Quelltext aller im Programm enthaltenen Module einschließlich aller zugehörigen Modulschnittstellen-Definitionsdateien sowie der zur Kompilation und Installation verwendeten Skripte. Als besondere Ausnahme jedoch braucht der verteilte Quelltext nichts von dem zu enthalten, was üblicherweise (entweder als Quelltext oder in binärer Form) zusammen mit den Hauptkomponenten des Betriebssystems (Kernel, Compiler usw.) geliefert wird, unter dem das Programm läuft – es sei denn, diese Komponente selbst gehört zum ausführbaren Programm.

Wenn die Verbreitung eines ausführbaren Programms oder von Objectcode dadurch erfolgt, dass der Kopierzugriff auf eine dafür vorgesehene Stelle

gewährt wird, so gilt die Gewährung eines gleichwertigen Zugriffs auf den Quelltext als Verbreitung des Quelltextes, auch wenn Dritte nicht dazu gezwungen sind, den Quelltext zusammen mit dem Objectcode zu kopieren.

4. Sie dürfen das Programm nicht vervielfältigen, verändern, weiter lizenzieren oder verbreiten, sofern es nicht durch diese Lizenz ausdrücklich gestattet ist. Jeder anderweitige Versuch der Vervielfältigung, Modifizierung, Weiterlizenzierung und Verbreitung ist nichtig und beendet automatisch Ihre Rechte unter dieser Lizenz. Jedoch werden die Lizenzen Dritter, die von Ihnen Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese die Lizenz voll anerkennen und befolgen.

5. Sie sind nicht verpflichtet, diese Lizenz anzunehmen, da Sie sie nicht unterzeichnet haben. Jedoch gibt Ihnen nichts anderes die Erlaubnis, das Programm oder von ihm abgeleitete Datenwerke zu verändern oder zu verbreiten. Diese Handlungen sind gesetzlich verboten, wenn Sie diese Lizenz nicht anerkennen. Indem Sie das Programm (oder ein darauf basierendes Datenwerk) verändern oder verbreiten, erklären Sie Ihr Einverständnis mit dieser Lizenz und mit allen ihren Bedingungen bezüglich der Vervielfältigung, Verbreitung und Veränderung des Programms oder eines darauf basierenden Datenwerks.

6. Jedes Mal, wenn Sie das Programm (oder ein auf dem Programm basierendes Datenwerk) weitergeben, erhält der Empfänger automatisch vom ursprünglichen Lizenzgeber die Lizenz, das Programm entsprechend den hier festgelegten Bestimmungen zu vervielfältigen, zu verbreiten und zu verändern. Sie dürfen keine weiteren Einschränkungen der Durchsetzung der hierin zugestandenen Rechte des Empfängers vornehmen. Sie sind nicht dafür verantwortlich, die Einhaltung dieser Lizenz durch Dritte durchzusetzen.

7. Sollten Ihnen infolge eines Gerichtsurteils, des Vorwurfs einer Patentverletzung oder aus einem anderen Grunde (nicht auf Patentfragen begrenzt) Bedingungen (durch Gerichtsbeschluss, Vergleich oder anderweitig) auferlegt werden, die den Bedingungen dieser Lizenz widersprechen, so befreien Sie diese Umstände nicht von den Bestimmungen dieser Lizenz. Wenn es Ihnen nicht möglich ist, das Programm unter gleichzeitiger Beachtung der Bedingungen in dieser Lizenz und Ihrer anderweitigen Verpflichtungen zu verbreiten, dann dürfen Sie als Folge das Programm überhaupt nicht verbreiten. Wenn zum Beispiel ein Patent nicht die gebührenfreie Weiterverbreitung des Programms durch diejenigen erlaubt, die das Programm direkt oder indirekt von Ihnen erhalten haben, dann besteht der einzige Weg, sowohl das Patentrecht als auch diese Lizenz zu befolgen, darin, ganz auf die Verbreitung des Programms zu verzichten.

Sollte sich ein Teil dieses Paragraphen als ungültig oder unter bestimmten Umständen nicht durchsetzbar erweisen, so soll dieser Paragraph seinem Sinne nach angewandt werden; im übrigen soll dieser Paragraph als Ganzes gelten.

Zweck dieses Paragraphen ist nicht, Sie dazu zu bringen, irgendwelche Patente oder andere Eigentumsansprüche zu verletzen oder die Gültigkeit solcher Ansprüche zu bestreiten; dieser Paragraph hat einzig den Zweck, die Integrität des Verbreitungssystems der freien Software zu schützen, das durch die Praxis öffentlicher Lizenzen verwirklicht wird. Viele Leute haben großzügige Beiträge zu dem großen Angebot der mit diesem System verbreiteten Software im Vertrauen auf die konsistente Anwendung dieses Systems geleistet; es liegt am Autor/Geber, zu entscheiden, ob er die Software mittels irgendeines anderen Systems verbreiten will; ein Lizenznehmer hat auf diese Entscheidung keinen Einfluss.

Dieser Paragraph ist dazu gedacht, deutlich klarzustellen, was als Konsequenz aus dem Rest dieser Lizenz betrachtet wird.

8. Wenn die Verbreitung und/oder die Benutzung des Programms in bestimmten Staaten entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann der Urheberrechtsinhaber, der das Programm unter diese Lizenz gestellt hat, eine explizite geographische Begrenzung der Verbreitung angeben, in der diese Staaten ausgeschlossen werden, so dass die Verbreitung nur innerhalb und zwischen den Staaten erlaubt ist, die nicht ausgeschlossen sind. In einem solchen Fall beinhaltet diese Lizenz die Beschränkung, als wäre sie in diesem Text niedergeschrieben.

9. Die *Free Software Foundation* kann von Zeit zu Zeit überarbeitete und/oder neue Versionen der *General Public License* veröffentlichen. Solche neuen Versionen werden vom Grundprinzip her der gegenwärtigen entsprechen, können aber im Detail abweichen, um neuen Problemen und Anforderungen gerecht zu werden.

Jede Version dieser Lizenz hat eine eindeutige Versionsnummer. Wenn in einem Programm angegeben wird, dass es dieser Lizenz in einer bestimmten Versionsnummer oder „jeder späteren Version“ *(„any later version“)* unterliegt, so haben Sie die Wahl, entweder den Bestimmungen der genannten Version zu folgen oder denen jeder beliebigen späteren Version, die von der *Free Software Foundation* veröffentlicht wurde. Wenn das Programm keine Versionsnummer angibt, können Sie eine beliebige Version wählen, die je von der *Free Software Foundation* veröffentlicht wurde.

10. Wenn Sie den Wunsch haben, Teile des Programms in anderen freien Programmen zu verwenden, deren Bedingungen für die Verbreitung anders sind, schreiben Sie an den Autor, um ihn um die Erlaubnis zu bitten.

Für Software, die unter dem Copyright der *Free Software Foundation* steht, schreiben Sie an die *Free Software Foundation*; wir machen zu diesem Zweck gelegentlich Ausnahmen. Unsere Entscheidung wird von den beiden Zielen geleitet werden, zum einen den freien Status aller von unserer freien Software abgeleiteten Datenwerke zu erhalten und zum anderen das gemeinschaftliche Nutzen und Wiederverwenden von Software im allgemeinen zu fördern.

Keine Gewährleistung

11. Da das Programm ohne jegliche Kosten lizenziert wird, besteht keinerlei Gewährleistung für das Programm, soweit dies gesetzlich zulässig ist. Sofern nicht anderweitig schriftlich bestätigt, stellen die Copyright-Inhaber und/oder Dritte das Programm so zur Verfügung, „wie es ist", ohne irgendeine Gewährleistung, weder ausdrücklich noch implizit, einschließlich – aber nicht begrenzt auf – Marktreife oder Verwendbarkeit für einen bestimmten Zweck. Das volle Risiko bezüglich Qualität und Leistungsfähigkeit des Programms liegt bei Ihnen. Sollte sich das Programm als fehlerhaft herausstellen, liegen die Kosten für notwendigen Service, Reparatur oder Korrektur bei Ihnen.

12. In keinem Fall, außer wenn durch geltendes Recht gefordert oder schriftlich zugesichert, ist irgendein Copyright-Inhaber oder irgendein Dritter, der das Programm wie oben erlaubt modifiziert oder verbreitet hat, Ihnen gegenüber für irgendwelche Schäden haftbar, einschließlich jeglicher allgemeiner oder spezieller Schäden, Schäden durch Seiteneffekte (Nebenwirkungen) oder Folgeschäden, die aus der Benutzung des Programms oder der Unbenutzbarkeit des Programms folgen (einschließlich – aber nicht beschränkt auf – Datenverluste, fehlerhafte Verarbeitung von Daten, Verluste, die von Ihnen oder anderen getragen werden müssen, oder dem Unvermögen des Programms, mit irgendeinem anderen Programm zusammenzuarbeiten), selbst wenn ein Copyright-Inhaber oder Dritter über die Möglichkeit solcher Schäden unterrichtet worden war.

Ende der Bedingungen

Anhang: Wie Sie diese Bedingungen auf Ihre eigenen, neuen Programme anwenden können

Wenn Sie ein neues Programm entwickeln und wollen, dass es vom größtmöglichen Nutzen für die Allgemeinheit ist, dann erreichen Sie das am bes-

ten, indem Sie es zu freier Software machen, die jeder unter diesen Bestimmungen weiterverbreiten und verändern kann.

Um dies zu erreichen, fügen Sie die folgenden Vermerke zu Ihrem Programm hinzu. Am sichersten ist es, sie an den Anfang einer jeden Quelldatei zu stellen, um den Gewährleistungsausschluss möglichst deutlich darzustellen; zumindest aber sollte jede Datei eine Copyright-Zeile besitzen sowie einen kurzen Hinweis darauf, wo die vollständigen Vermerke zu finden sind.

```
<Program name and short description>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public
License along with this program; if not, write to the Free
Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,
MA 02111-1307, USA.
```

Auf Deutsch:

```
<Programmnamen und einer kurzen Beschreibung>

Copyright (C) <Jahr> <Name des Autors>

Dieses Programm ist freie Software. Sie können es unter den
Bedingungen der GNU General Public License, wie von der Free
Software Foundation veröffentlicht, weitergeben und/oder
modifizieren, entweder gemäß Version 2 der Lizenz oder (nach
Ihrer Option) jeder späteren Version.

Die Veröffentlichung dieses Programms erfolgt in der Hoffnung,
dass es Ihnen von Nutzen sein wird, aber OHNE IRGENDEINE
GARANTIE, sogar ohne die implizite Garantie der MARKTREIFE oder
der VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. Details finden
```

```
Sie in der GNU General Public License.

Sie sollten eine Kopie der GNU General Public License zusammen
mit diesem Programm erhalten haben. Falls nicht, schreiben Sie
an die Free Software Foundation, Inc., 59 Temple Place,
Suite 330, Boston, MA 02111-1307, USA.
```

Fügen Sie auch einen kurzen Hinweis hinzu, wie Sie elektronisch und per Brief erreichbar sind.

Wenn Ihr Programm interaktiv ist, sorgen Sie dafür, dass es nach dem Start einen kurzen Vermerk ausgibt:

```
Gnomovision version 69, Copyright (C) <year> <name of author>

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type
'show w'. This is free software, and you  are welcome to
redistribute it under certain conditions; type 'show c' for
details.
```

Auf Deutsch:

```
Gnomovision Version 69, Copyright (C) <Jahr> <Name des Autors>

Für Gnomovision besteht KEINERLEI GARANTIE; geben Sie
'show w' für Details ein. Gnonovision ist freie Software, die
Sie unter bestimmten Bedingungen weitergeben
dürfen; geben Sie 'show c' für Details ein.
```

Die hypothetischen Kommandos `show w` und `show c` sollten die entsprechenden Teile der GNU-GPL anzeigen. Natürlich können die von Ihnen verwendeten Kommandos anders heißen als `show c` und `show c`; es könnten auch Mausklicks oder Menüpunkte sein – was immer am besten in Ihr Programm passt.

Soweit vorhanden, sollten Sie auch Ihren Arbeitgeber (wenn Sie als Programmierer arbeiten) oder Ihre Schule einen Copyright-Verzicht für das Programm unterschreiben lassen. Hier ein Beispiel. Die Namen müssen Sie natürlich ändern.

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
program 'Gnomovision' (which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1st April 1989 Ty Coon, President of Vice
```

Auf Deutsch:

```
Die Yoyodyne GmbH erhebt keinen urheberrechtlichen Anspruch auf
das von James Hacker geschriebene Programm 'Gnomovision' (einem
Schrittmacher für Compiler).

Unterschrift von Ty Coon1. April 1989 Ty Coon, Vizepräsident
```

Diese *General Public License* gestattet nicht die Einbindung des Programms in proprietäre Programme. Ist Ihr Programm eine Funktionsbibliothek, so kann es sinnvoller sein, das Binden proprietärer Programme mit dieser Bibliothek zu gestatten. Wenn Sie dies tun wollen, sollten Sie die GNU Library General Public License anstelle dieser Lizenz verwenden.

Literaturverzeichnis

[1] *SuSE Linux* (*User Guide*). SuSE, 2. Auflage ©2003 .

[2] EDWARD C. BAILEY. *Maximum RPM*. ©1997 . ISBN 1-888172-78-9.

[3] BRYAN COSTALES, ERIC ALLMAN, NEIL RICKERT. *sendmail*. ©1993 . ISBN 1-56592-056-2.

[4] WERNER ALMESBERGER. *LILO User's guide*. `file:///usr/share/doc/lilo/user.dvi`.

[5] OLAF KIRCH. *LINUX Network Administrator's Guide*. ©1995 . ISBN 1-56592-087-2.

[6] SEBASTIAN HETZE, DIRK HOHNDEL, MARTIN MÜLLER, OLAF KIRCH. *Linux Anwenderhandbuch*. 6. Auflage ©1996 . ISBN 3-929764-05-9.

[7] SIMON GARFINKEL, GENE SPAFFORD. *Practical UNIX Security*. ©1993 . ISBN 0-937175-72-2.

[8] CRAIG HUNT. *TCP/IP Netwerk Administration*. ©1995 . ISBN 3-930673-02-9.

[9] TIM O'REILLY, GRACE TODINO. *Managing UUCP and Usenet*. ©1992 . ISBN 0-937175-93-5.

[10] MATT WELSH. *Linux Installation and Getting Started*. 2. Auflage ©1994 . ISBN 3-930419-03-3.

[11] LINDA LAMB. *Learning the vi Editor*. ©1990 . ISBN 0-937175-67-6.

[12] MATT WELSH, LARS KAUFMAN. *Running Linux*. ©1995 O'Reilly. ISBN 1-56592-100-3.

[13] JÜRGEN SCHNEIDERER. *Sicherheit Kostenlos – Firewall mit Linux*. ©1998 iX.

[14] MICHAEL KIENLE. *TIS: Toolkit für anwendungsorientie Firewall-Systeme*. ©1995 iX.

[15] ULRICH KUNITZ. *Sicherheit fast kostenlos: Einrichtung eines kostenlosen Firewall-Systems*. ©1995 iX.

[16] WILLIAM R. CHESWICK, STEVEN M. BELLOVIN. *Firewalls und Sicherheit im Internet*. ©1996 Addison Wesley. ISBN 3-89319-875-x.

[17] BRENT CHAPMAN, ELISABETH D. ZWICKY. *Einrichten von Internet Firewalls* (*Sicherheit im Internet gewährleisten*). ©1996 O'Reilly. ISBN 3-930673312.

[18] CLIFFORD STOLL. *Kuckucksei. Die Jagd auf die deutschen hacker, die das Pentagon knackten*. ©1998 Fischer-TB. Verlag. ISBN 3-596139848.

[19] BRIAN TUNG. *Kerberos: A Network Authentication System*. ©1999 Fischer-TB. Verlag. ISBN 0-201-37924-4.

[20] CHIN FANG, BOB CROSSON, ERIC S. RAYMOND. *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*. ©1993 .

[21] SEBASTIAN HETZE, DIRK HOHNDEL, MARTIN MÜLLER, OLAF KIRCH. *Linux Anwenderhandbuch*. 6. Auflage ©1996 LunetIX Softfair. ISBN 3-929764-05-9.

[22] MATTHIAS KETTNER. *Fehlerdiagnose und Problembehebung unter Linux*. ©2004 SUSE PRESS Verlag. ISBN 3-89990-051-0.

Index

Symbole

.local als Top-Level-Domain 186
64-bit Linux 217
- Kernel-Spezifika 222
- Laufzeit-Unterstützung 218
- Softwareentwicklung 219

A

ACLs (Access Control Lists) 765–778
- DNS 513
- Kerberos 739
ACPI 393
Adressen
- IP 458
- MAC 458
Apache 581–608
- apxs 588
- Beispielumgebung 269
- CGI 596
- Content Negotiation 585
- DocumentRoot 590
- Fehlerbehandlung 585
- Flags 589
- Installation 587–588
- Konfiguration 589–594
- logging 593, 594
- Module 584
· aktivieren 589
· laden 590
· mod_perl 598
· mod_php4 600
· mod_python 601
· mod_ruby 601
- permissions 591
- Sicherheit 605–606
- Squid 674
- SSI 596
- SSI (Server Side Includes) 593
- Standardseite 583
- starten 587
- Threads 586
- Troubleshooting 606
- Virtual Hosts 584, 601–605
- Zugriffsrechte 605
APM 393
Apple
- Netatalk 646
Arbeitsspeicher 273
ATA-RAID-Controller ..... *siehe* Hardware, Promise-Controller
Authentifizierung
- PAM 443–450

B

Backup 71
- Erstellen mit YaST 109
- Wiederherstellen 109
bash
- /etc/profile 269
Befehl
- chown 187
- head 187
- nice 187
- rpm 190
- rpmbuild 191
- sort 187
- tail 187
Befehle
- apm 399
- cdrecord 252
- cvs 611, 618
- dd 144

- depmod 260
- e2fsck 801
- ether-wake 419
- fdformat 143
- fonts-config 312
- getfacl 771
- grub 227
- hotplug 349
- hwinfo 260, 350
- insmod 260
- kadmin 734
- kinit 740
- kstash 733
- ktutil 743
- ldapadd 535
- ldapdelete 537
- ldapmodify 536
- ldapsearch 537, 746
- lilo 238
- lp 78
- lsmod 261
- modinfo 261
- modprobe 260
- rawwrite 142
- rawwritewin 142
- rmmod 260
- rsync 612, 625
- scp 716
- setfacl 772
- sftp 717
- slptool 500
- smbpasswd 642
- ssh 716
- ssh-agent 719
- ssh-keygen 719
- svn 611, 622
- syslinux 251
- udev 355
- unison 610, 616

Benutzer
- Probleme beim Anlegen 479
- Verwaltung mit YaST 103

Bildschirm
- Auflösung 309
- SuSE-Bildschirm deaktivieren .. 139

Bildschirmeinrichtung 81
BIND ..... *siehe* DNS
BIOS
- Bootreihenfolge 8
- Virus Protection 139
- Wake on LAN (WOL) 417

Bluetooth 384
- hciconfig 387
- hcitool 387
- opd 389
- pand 388
- sdptool 387

Bootdiskette 110, 144, 225, 239
- Erzeugen mit dd 143
- Erzeugen mit rawrite 142

Booten 289, 801, 807
- Ablauf 224
- Bootmanager 225
- GRUB 227–238
- initial ramdisk 275–280
- Konzept 225, 289
- LILO 237
- Methoden 139
- Rechner bleibt hängen .. *siehe* BIOS, Virus Protection
- von CD 8
- von CD2 145
- von Disketten 141

Bootkonfiguration 34
Bootloader
- GRUB 227
- LILO 237, 238
- Ort 247
- Typ 247
- YaST 244–248
- ZIPL 252

Bootmanager 223
- GRUB 225
- Windows NT 225

Bootsektor 224

C

cards
- ISDN 491

CD-ROM-Laufwerk
- Unterstützung durch Linux 145

CD-ROM-Laufwerke
- ATAPI 146

CDs
- Booten 8

chown 187
CID-keyed Fonts 318
CJK 285
Cold Standby 434
Coldplug 352
Compose *siehe* Tastaturbelegung, Compose
Concurrent Version System ..... *siehe* CVS
Core-Dateien 272
cpuspeed 407
Crash 801, 807
cron 270

CVS 611, 618

D

Dateien
- synchronisieren 609–631
  - · CVS 611
  - · mailsync 612
  - · rsync 612
  - · subversion 611
  - · unison 610

Dateisystem 422–431
- Access Controll Lists 766–778
- Beschränkungen 430
- e2fsck 801
- Ext2 423–424
- Ext3 424–425
- FHS 268
- JFS 427
- LFS 430–431
- Rechte 271
- ReiserFS 426
- reiserfsck 807
- Termini 422
- TeX 268
- XFS 427–429

Dateisysteme
- ext2 26
- ext3 26
- FAT 28
- JFS 26
- NTFS 28, 30
- ReiserFS 26
- sysfs 348

Deinstallation
- GRUB 249
- LILO 244, 249
- Linux 249
- Squid 665

DENIC 502
depmod 260
Device Nodes
- udev 355

DHCP
- Konfiguration mit YaST 569
- Server-Konfiguration 564
- statische Adressvergabe 566

Diskette
- Booten von 225
- formatieren 143

Distributed Replicated Block Device .. *siehe* DRBD

DNS 461, 502
- Forwarding 503
- Konfiguration 98
- Logging 506
- Mail Exchanger 462
- NIC 462
- Optionen 505
- Problemanalyse 503
- Squid und 665
- Starten 502
- top level domain 462
- umgekehrte Adress-Auflösung . 511
- Zonen 506
- Zonendateien 508

Domain 475
Domain Name System ..... *siehe* DNS
DRBD 439
Druck-System ..... *siehe* Spool-System
Drucken 74–323
- Anschluss 76
- Anwendungsprogramme 78
- CUPS 78
- Druckertreiber 76
- Einrichtung mit YaST 75
- Fehlerbehebung 78
- Fehlersuche
  - · Netzwerk 341
- GDI-Drucker 339
- Ghostscript-Treiber 76
- Kommandozeile 78
- kprinter 78
- Netzwerk
  - · Fehlersuche 341
- PPD-Datei 76
- Probleme 78
- Schnittstelle 76
- Warteschlangen 76
- xpp 78

Druckerkonfiguration
- Update 190

Drucksystem
- Update 324

E

E-Mail
- Konfiguration 100

e2fsck 801
Eingabemethode
- CJK 285

Einwahl
- smpppd 656

Emacs 274
Erstinstallation
- Bootdiskette erstellen
  - · DOS 141

· Linux, UNIX 143
- Booten von CD2 145
- Booten von Diskette 144
- künftige Boot-Methode 139
- linuxrc 126
- Startbildschirm 137
ESA Native Installation
- IPL 37

F

FAT-Dateisystem 28
fdisk 249
Fehlermeldung
- bad interpreter 31
- Permission denied 31
Festplatten
- DMA 92
FHS (File System Hierarchy Standard) . 268
Fileserver 98
Firewall 107, 705
- Squid 672
Font-Systeme 313
- CID-keyed Fonts 318
- X11 Core-Fonts 316
- Xft 313
Fonts 313
- CID-keyed 318
- X11 Core 316
- Xft 313
free 273
FTP-Server 268
- Beispielumgebung 268
Funkverbindung
- Bluetooth 384

G

GDT RAID5-Controller .... *siehe* ICP Vortex
GNU Emacs ..... *siehe* Emacs
GPL 813
Grafik
- 3D 318–321
· Diagnose 319
· Installationssupport 320
· SaX2 319
· Support 318
· Testen 320
· Treiber 318
· Troubleshooting 320
- Device-Identifier 310
- Farbtiefe 309
- id 319
Grafische Oberfläche 81–91
Grafischer Hintergrund ..... *siehe* SUSE-Bildschirm, deaktivieren
GRUB 227
- /etc/grub.conf 235
- Bootmenü 228
- Bootpasswort 236
- deinstallieren 249
- Gerätenamen 230
- GRUB-Shell 235
- Partitionsnamen 230
- Troubleshooting 237
Gruppenverwaltung 104

H

HA
- Cold Standby 434
- DRBD 439
- Failover 434
- heartbeat 438
- High Availability Cluster 440
- Hot Standby 435
- Linux Virtual Server 439
- Load Balancing 435
- RAID 438
- rsync 438
- SPOF 434
- STONITH 435
- Warm Standby 434
HA (High Availability) 433–441
Hardware
- CD-ROM 73
- CD-ROM-Laufwerke
· ATAPI 146
- DASD 74
- Festplatten-Controller 80
- Informationen 92
- Promise-Controller 179
- SCSI-Geräte
· Konfiguration ändern 147
- ZFCP 97
hciconfig 387
hcitool 387
head 187
heartbeat 438
High Availability Cluster 440
Hilfe
- Info 271
- Manual-Pages 271
- Texinfo 271
- Tkinfo 271
- XInfo 271
Hintergrund

- grafischer ... *siehe* SUSE-Bildschirm, deaktivieren
Hochverfügbarkeit ..... *siehe* HA, *siehe* HA
Hostname 98
Hot Standby 435
Hotplug 496
- Agent 349
· Geräte 349
· PCI 350
· Schnittstellen 350
· USB 350
- Blacklist 351
- Eventrecorder 353
- Events 349
- Fehleranalyse 352
- Gerätenamen 351
- Map-Dateien 350
- Module
· automatisch laden 350
- Netzwerkgeräte 351
- PCI 351
- Protokoll-Dateien 352
- Whitelist 351
hwinfo 350

I

I18N 286
IBM S/390 und zSeries
- Installation
· Rettungssystem 208
- Rettungssystem 208
ICP Vortex-Controller
- Installation schlägt fehl 133
IDE-Festplatte
- ATA-RAID-Controller ..... *siehe* Hardware, Promise-Controller
inetd 102
init 290
- Skripte 293
- Skripte hinzufügen 296
initial ramdisk (initrd) 275
insmod 260
Installation
- GRUB 227
- Kernel 263
- LILO 244
- Pakete 192
- textbasiert, mit YaST 137
- via FTP 141
- via Netzwerk 141
- via NFS 141
- via PCMCIA 371
- VNC 136
- YaST 7–50
Installationsserver einrichten 166
Installationssupport
- 3D-Grafikkarten 320
Internet
- DSL 489
- ISDN 491
- Proxy ..... *siehe* Squid
- smpppd 656
- TDSL 491
- Webserver ..... *siehe* Apache
IP-Adressen 458
- IPv6 ..... 463, 496
- Namensauflösung 461, 502
- Netzmasken 459
- Netzwerkklassen 459
- privater Adressbereich 461
IPsec
- YaST 694
IrDA 381
iSCSI 163

K

Kabelmodem 484
Karten
- Grafik 84
- Netzwerk 482
- Sound 95
Kerberos 721
- Authenticator 722
- Clientkonfiguration 735–738
- Credential 722
- Host-Principals 741
- Installation und Administration 729–748
- KDC 732–735
- Konfiguration von SSH 743
- LDAP und Kerberos 745–748
- Master Key 733
- Mutual Authentication 723
- PAM-Unterstützung 743
- Principal 723, 734
- Protokollfunktion 732
- Realm 729, 733
- Replay 723
- Session Key 723
- Ticket 722
- Zeitsynchronisation 731
Kernel 255
- Daemon 261
- installieren 263
- Kompilierung 255
- Konfiguration 257

- Module 259
  · übersetzen 263
  · depmod 260
  · insmod 260
  · modinfo 261
  · modprobe 260, 261
  · modprobe.conf 184
  · Netzwerkkarten 481
  · rmmod 260
- Module Loader 261
- Neuheiten der Version 2.6 184

Kernel too big 262
Kmod ..... *siehe* Kernel Module Loader
Kodierung
- UTF-8 186

Konfiguration
- Apache 589–594
- Benutzer 103
- Bootloader
  · GRUB 227
  · LILO 240
- CD-ROM 73
- DASD 74
- DHCP 564–576
- DNS 98, 502
- Drucken 74
- DSL 489
- E-Mail 100
- Festplatten (DMA) 92
- Festplatten-Controller 80
- Firewall 107
- Grafikkarten 84
- Gruppenverwaltung 104
- Hardware 73
- hwinfo 350
- hwup 350
- IPv6 496
- ISDN 491
- Kabelmodem 484
- Kerberos 729–748
- Kernel 255–266
- Kontrollzentrum 53
- Laptops 361, 364–373
- LDAP 528–551
- LVM 152
- Mailserver 101
- Maus 93
- Modem 486
- Netatalk 646–653
- Netzwerk 98–100, 482, 498
- NFS 98, 558–563
- NIS 554–557
- NTP
  · Client 99
- Routing 100, 497
- Runlevel 291
- Samba 636–646
  · Client 99
  · Server 98
- Scanner 93
- Sicherheit 103–107
- Soft-RAID 160
- Software 53–70
- Soundkarten 95
- Sprache 116
- Squid 666
- SSH 715
- SuSEfirewall2 710–714
- System 51–119
- Systemdienste 102
- Systemeinstellungen 299
- T-DSL 491
- Tastenbelegung 117
- X 81
- Zeitzone 116
- ZFCP 97

Konfigurationsdateien 473
- /boot/grub/menu.lst 228
- /etc/HOSTNAME 480
- /etc/conf.modules ..... *siehe* /etc/modprobe.conf
- /etc/dhcpd.conf 564
- /etc/exports 560, 562
- /etc/group 179
- /etc/grub.conf 235
- /etc/gshadow 188
- /etc/host.conf 476, 477
- /etc/hosts 476
- /etc/hotplug 348
- /etc/inittab 290
- /etc/lilo.conf 240
- /etc/modprobe.conf 261
- /etc/modules.conf ..... *siehe* /etc/modprobe.conf
- /etc/named.conf 504
- /etc/netatalk/netatalk.conf 648
- /etc/networks 476
- /etc/nscd.conf 479
- /etc/nsswitch.conf 477, 544
- /etc/openldap/slapd.conf 528
- /etc/passwd 179
- /etc/profile 269
- /etc/resolv.conf 273, 474
- /etc/slp.reg.d 499
- /etc/squid/squid.conf 666, 672, 675
- /etc/squidguard.conf 677

- /etc/sysconfig/network/ifroute-* .. 497
- /etc/sysconfig/network/routes 497
- apache2 589
- asound.conf 97
- fstab 31
- hotplug 352
- httpd.conf 589, 590
- modprobe.conf 97, 184
- modules.conf 96
- pam_unix2.conf 543
- sysconfig 116
Konsole
- virtuell 284
Kontrollzentrum 53

L

L10N 286
LAN 481
Laptop 361
LDAP 521–553
- Access Control Information 531
- Benutzer verwalten 550
- Daten ändern 536
- Daten durchsuchen 537
- Daten hinzufügen 533
- Daten löschen 537
- Gruppen verwalten 550
- Kerberos und LDAP 745–748
- Konfiguration mit YaST 537
- ldapadd 533
- ldapdelete 537
- ldapmodify 536
- ldapsearch 537
- Server
  · Konfiguration mit YaST 537
- Serverkonfiguration 528
- Verzeichnisbaum 525
- YaST LDAP Client
  · Templates 545
- YaST LDAP-Client 543
  · Module 545
LFS (Large File Support) 430
Lightweight Directory Access Protocol *siehe* LDAP
LILO 237, 238
- deinstallieren 249
- Grundlagen 238
- Installation 244
- Konfiguration 240
Linux
- deinstallieren 249
- Update 177
Linux Virtual Server 439
linuxrc 126
linuxthreads 185
Lizenz ..... *siehe* GPL
Load Balancing 435
Local Area Network ..... *siehe* LAN
Locale
- UTF-8 186
Logdateien
- apache2 ..... 594, 606
- boot.msg 118
- httpd 592, 594, 606
- log 106
- messages 118
Logging
- Anmeldeversuche 106
LPAR Installation
- IPL 37
LSB (Linux Standard Base) 268
- Pakete installieren 191
lsmod 261
LVM ..... *siehe* YaST, LVM

M

Mac OS 646
Mailserver
- Konfiguration 101
mailsync 612, 627
Manpages ..... *siehe* Hilfe, Manual-Pages
Masquerading 705
Master Boot Record ..... *siehe* MBR
Maus
- Konfiguration 93
MBR .... 224, 239, *siehe* Master Boot Record
mkinitrd 278
Modeline 311
Modems
- YaST 486
modinfo 261
modprobe 260
Modul
- hwinfo 259
- Laden 128
- Parameter 129
- Umgang 260
Moduldiskette 110
Multi_key ..... *siehe* Tastaturbelegung, Compose
Multicast-DNS 186

N

Name Service Cache Daemon 479
Nameserver 475, 502

- BIND 502
Netatalk 646
NetBIOS 635
- Namensdienst 635
Network File System ..... *siehe* NFS
Network Information Service ..... *siehe* NIS
Netzwerk 453
- Broadcastadresse 461
- DNS 461
- IP-Adressen 458
- Kerberos 721
- Konfiguration 98
· IPv6 496
- Konfigurationsdateien 473
- Localhost 461
- manuelle Konfiguration 472
- Netzmasken 459
- Netzwerkbasisadresse 460
- Routing 100, 458, 459, 497
- SLP 498
- Test 481
- YaST 482
NFS 557
- Client 98, 557
- exportieren 559, 560
- importieren 558
- mount 559
- mountd 560
- Server 98, 557
nfsd 560
NGPT 185
nice 187
NIS 553–557
- Client 556
- Master 554–556
- Slave 554–556
Notebook ..... *siehe* Laptop
- ACPI 393
- APM 393
- IrDA 381
- PCMCIA 496
- Powermanagement 393
- SCPM 373
Notfallsystem 280
NPTL 185
NSS (Name Service Switch) 478
NTFS-Dateisystem 28
NTP
- Client 99

O

opd 389
OpenGL 318–321
- Testen 320
- Treiber 318
OpenLDAP ..... *siehe* LDAP
OpenSSH ..... *siehe* SSH

P

Pakete
- build 200
- deinstallieren 192
- installieren 192
- kompilieren 191, 198
- LSB 191
- Paket-Manager 190
- Paketformat 190
Paketfilter ..... *siehe* SuSEfirewall2
PAM 443–450
pand 388
Partitionen
- /etc/fstab 31
- Erstellen 18, 24, 25
- LVM 26
- Parameter 25
- RAID 26
- Swap 26
- Typen 20
- Windows- anpassen 27
Partitionieren
- Experte 148
- fdisk 249
- Partitionstabelle 224
- Swap 149
Partitionierer ..... *siehe* YaST,Partitionierer
PCMCIA 362, 496
- Cardmanager 363
- Fehlerbehebung 366
- Hilfsprogramme 372
- Installation via 371
- IrDA 381
- ISDN 365
- Konfiguration 364
- Modem 365
- Netzwerkkarten 365
- SCSI 366
PGP 191
Pluggable Authentication Modules ... *siehe* PAM
portmap 560
Portscan 674
PostgreSQL
- Update 179
Powermanagement 393, 407–413
- ACPI 408
- APM 408

- cpufrequency 407
- cpuspeed 407
- Ladezustand 409
- Powersave 407
- YaST 413
Powersave 407
- Konfiguration 407
Profilmanager 114
Programme
- kompilieren 198
Programmieren
- Core-Dateien 272
Promise-Controller ..... *siehe* Hardware, Promise-Controller
Protokoll-Dateien 270
Protokolle
- ICMP 455
- IGMP 455
- TCP/IP 454
- UDP 455
Proxy ..... *siehe* Squid

Q

Quellen
- kompilieren 198

R

RAID 438
RAID-Controller
- ATA ..... *siehe* Hardware, Promise-Controller
rccoldplug 352
Rechner bleibt hängen .... *siehe* BIOS, Virus Protection
Rechte ..... *siehe* Dateisystem,Rechte
reiserfsck 807
Resolver-Bibliothek
- .local als Top-Level-Domain 186
Rettungsdiskette 110
Rettungssystem 11, 280
- benutzen 283
- Rettungsdiskette 280
- starten 281
Reverse lookup ..... *siehe* DNS
rmmod 260
Routing 100, 458, 497
- Netzmasken 459
- routes 497
- statisch 497
RPC-Mount-Daemon 560
RPC-NFS-Daemon 560
RPC-Portmapper 558, 560
RPM 190
- Patches 194
- rpmnew 192
- rpmorig 192
- rpmsave 192
rpmbuild 191
rsync 438, 612, 625
Runlevel 291
- Editor 114–115
- Runlevel-Editor 297
- Voreinstellung 115
- Wechseln 115
- wechseln 292

S

Samba 634–646
- Client 99
- Freigaben (Shares) 638
- Security Level 640
- Server 98
- Serverkonfiguration 636
SaX 81
SaX2
- Multihead 87
Scannen
- Fehlerbehebung 94
- Konfiguration 93
SCPM 114, 373
- Einrichten 375
- Profile verwalten 376
SCSI-Geräte
- Konfiguration ändern 147
SCSI-Gerätedateien
- Namen zuweisen 147
sdptool 387
Sercvice Location Protocol ..... *siehe* SLP
Server
- YOU 170
SGML
- Dateisystem nach FHS 190
Sicherheit 748
- Firewall 107, 705
- Konfiguration 103–107
- Squid 660
- SSH 715–721
Skript
- init.d
  · network 480
  · nfsserver 480
  · portmap 480
  · postfix 480
  · squid 664
  · xinetd 480

· ypbind 481
· ypserv 481
- modify_resolvconf 475
SLP 498
- Dienste registrieren 499
- Konqueror 501
- SLP-Browser 500
- slptool 500
SLP-Browser 500
slptool 500
SMB ..... *siehe* Samba
smpppd 656
Soft-RAID ..... *siehe* YaST,Soft-RAID
Software
- Entwicklung
· SUSE SDK 72
- Installieren 59–66
- Löschen 59–66
sort 187
Sound
- YaST-Konfiguration 95
Soundfonts
- YaST-Installation 96
Speicher 273
SPOF (Single Point of Failure) 434
Spool-System 323
Sprache 116
Squid 659
- Access Controls 675
- Apache 674
- Cache-Größe 663
- cachemgr.cgi 674
- Caches 661
- Calamaris 678
- CPU 664
- DNS 665
- Eigenschaften 660
- Festplatte 662
- Firewall 672
- Konfiguration 666
- Logdatei 665
- Objekte speichern 662
- Proxy-Cache 660
- RAM 663
- Rechte 669
- SARG 678
- Sicherheit 660
- squidGuard 676
- Starten 664
- Statistik 674
- Transparenter Proxy 671
- Verzeichnisse 664
- Zugriffskontrolle 669
SSH 715–721
- Authentifizierung 719
- scp 716
- sftp 717
- ssh-agent 719
- sshd 717
Startprotokoll 118
Startskipt
- rccoldplug 352
Startskripte
- boot.udev 360
Startup-Skripten ..... *siehe* Skript, init.d
STONITH 435
subfs
- Wechselmedien 190
Subversion 622
subversion 611
Support-Anfrage 117
SuSE Linux 267
- Besonderheiten 267
- Installation 126
- Tastaturbelegung 285
SUSE SDK 72
SuSEconfig 299
SuSEfirewall2 705
sysconfig 299
Sysconfig-Editor 116
System
- Konfiguration 51–119
- sicherheit 105
- Sprache 116
- Update 68
System is too big 262
System-Update 177
Systemdienste 102
Systeminformationen 127
Systemprotokoll 118
Systemreparatur 203

T

tail 187
Tastatur
- Konfiguration 117
Tastaturbelegung 285
- Compose 285
TCP/IP 454
- Dienste 454
- ICMP 455
- IGMP 455
- Pakete 455, 457
- Schichtenmodell 455
- TCP 454
- UDP 455

Telefonanlage 493
Testseite drucken 77
Thread-Paket
- NPTL 185
Treiber-CD 119
TrueType ..... *siehe* X11, TrueType-Font

U

udev 355
- Automatisierung 357
- Massenspeicher 359
- Regeln 356
- Reguläre Ausdrücke 357
- Schlüssel 358
- Startskript 360
- sysfs 358
- udevinfo 358
- YaST 360
UDP ..... *siehe* TCP
ugidd 560
ulimit 272
umgekehrte Adress-Auflösung
- reverse lookup 511
unison 610, 616
Update 177
- /etc/skel 183
- Drucksystem 324
- online 54–58
- passwd/group prüfen 179
- Patch-CD 58
- profile 183
- YOU-Server 170
USB-Stick
- Booten von 225
UTF-8
- Kodierung 186

V

Vernetzung 453
Virtuelle Konsolen 284
- Umschalten 115
virtueller Bildschirm 309
Virtueller Speicher 26
Virus Protection ..... *siehe* BIOS, Virus Protection
Virus-Warnung 139
VNC
- Installation 136
VPN
- FreeS/WAN 694
- FreeS/WAN-Client 698
- FreeS/WAN-Server 695
- Windows-Client 701
- YaST 694

W

Wake on Lan (WOL) 416
Warm Standby 434
Webserver ..... *siehe* Apache
Wechselmedien
- subfs 190
whois 463
Windows 634
- NT Bootmanager 225
- SMB 634

X

X ..... *siehe* X11
- Konfiguration 81
- Multihead 87
X Window System ..... *siehe* X11
X.509-Zertifikat 682
X.509-Zertifizierung
- Grundlagen 680
- Rückrufliste 683
- Repository 684
- YaST 680
X11 305
- CID-keyed Fonts 318
- Font 312
- Font-Systeme 313
- Optimierung 306
- Treiber 310
- TrueType-Font 312
- X11 Core-Fonts 316
- Xft 313
- xft 312
- Zeichensatz 312
X11 Core-Fonts 316
XF86Config
- Clocks 309
- Depth 309
- Device 308–310
- Files 307
- InputDevice 307
- Modeline 307
- modeline 309
- Modes 307, 309, 311
- Monitor 307, 309, 311
- Screen 308
- ServerFlags 307
- ServerLayout 308
- Subsection
· Display 309
- Virtual 310
Xft 313

XML
- Dateisystem nach FHS 190

Y

YaST
- 3D 318
- Backup 71, 109
- Benutzerverwaltung 103
- Bildschirmeinrichtung 81
- Boot from Harddisk 11
- Boot-Modus 34
- Bootdiskette 110
- CA-Modul 684
- CD-ROM 73
- DASD 74
- DHCP 569
- DMA 92
- Drucken 74
- DSL 489
- E-Mail 100
- EVMS 113
- Festplatten-Controller 80
- Firewall 107
- Grafikkarte 81
- Grafikkarten 84
- Grafische Oberfläche 81–91
- Gruppenverwaltung 104
- Hardware 73
- Hardware-Informationen 92
- Hostname und DNS 98
- Installation 7–50
- Installation - ACPI Disabled 11
- Installationsmodus 15
- Installationsquelle ändern 53
- Installationsserver 166
- Installationsumfang 32
- Installationsvorschlag 16
- IPsec 694
- ISDN 491
- Kabelmodem 484
- Konfiguration 51–119
- Kontrollzentrum 53
- LDAP-Client 543
- LDAP-Server 537
- LVM 113
- LVM (Logical Volume Manager) 153
- Mailserver 101
- Manual Installation 11
- Maus 18, 93
- Memory Test 11
- Modem 486
- ncurses 119
- Netzwerk-Konfiguration 98–100
- Netzwerkkarte 482
- Netzwerkkonfiguration 40
- NFS-Client 98, 558
- NFS-Server 98, 559
- NIS-Client 44, 556
- NIS-Server 554
- NTP
  - Client 99
- Online-Update 54–58
- Online-Update über die Konsole 122
- Paket-Manager 60
- Paketabhängigkeiten 34
- Paketzustände 63
- Partitionieren 18, 24
- Partitionierer 152
- Patch-CD-Update 58
- Powermanagement 413
- Profilmanager 114
- rc.config 116
- Rettungssystem 11
- Root-Passwort 39
- Routing 100
- Runlevel-Editor 297
- Runlevels 115
- Safe Settings 11
- Samba
  - Cient 99
  - Server 98
- Scanner 93
- SCPM 114
- Sendmail 100
- Sicherheit 103–107
- SLP-Browser 500
- Soft-RAID 160
- Software 53–70
- Software-Updates 42
- Soundkarten 95
- Speicherplatz 20
- Sprachauswahl 13
- Sprache 116
- Starten 8, 52
- Support-Anfrage 117
- Sysconfig-Editor 116, 301
- Systemreparatur 203
- Systemsicherheit 105
- Systemstart 8
- T-DSL 491
- Tastatur 17
- Tastaturbelegung 117, 119
- Textmodus 119–124
- Treiber-CD des Herstellers 119
- Update 68
- VPN 694

- Wake on LAN (WOL) 418
- X.509-Zertifizierung 680
  · Allgemeines Server-Zertifikate importieren 693
  · CA-Objekte als Datei exportieren 692
  · CA-Objekte nach LDAP exportieren 691
  · Client und Server-Zertifikate 688
  · CRLs erzeugen 690
  · Root-CA 685
  · Standardwerte verändern 688
  · Sub-CA 686
  · Zertifikate auf Floppy exportieren 693
  - YOU 54–58
  - YOU-Server 170
  - ZCFP 97
  - Zeitzone auswählen 116
YOU 170
YP ..... *siehe* NIS

Z

z/VM Installation
  - IPL installiertes System 37
Zeitzone 116
ZIPL 252
  - Benutzung 252
  - Konfigurationsdatei 253